Workgroup:
Oblivious HTTP Application Intermediation
Internet-Draft: draft-ietf-ohai-svcb-config-07
Published: 6 October 2023
Intended Status: Standards Track
Expires: 8 April 2024
Authors: T. Pauly
Apple Inc.
T. Reddy
Nokia

Discovery of Oblivious Services 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 using Oblivious HTTP, by offering an Oblivious Gateway Resource through which to access the target. This document also defines a mechanism to learn the key configuration of the discovered Oblivious Gateway Resource.

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-ietf-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/. Subscribe at https://www.ietf.org/mailman/listinfo/ohai/.

Source for this draft and an issue tracker can be found at https://github.com/ietf-wg-ohai/draft-ohai-svcb-config.

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 8 April 2024.

Table of Contents

1. Introduction

Oblivious HTTP [OHTTP] allows clients to encrypt messages exchanged with an Oblivious Target Resource (target). The messages are encapsulated in encrypted messages to an Oblivious Gateway Resource (gateway), which offers Oblivious HTTP access to the target. The gateway is accessed via an Oblivious Relay Resource (relay), which proxies the encapsulated messages to hide the identity of the client. Overall, this architecture is designed in such a way that

the relay cannot inspect the contents of messages, and the gateway and target cannot learn the client's identity from a single transaction.

Since Oblivious HTTP deployments typically involve very specific coordination between clients, relays, and gateways, the key configuration is often shared in a bespoke fashion. However, some deployments involve clients discovering targets and their associated gateways more dynamically. For example, a network might operate a DNS resolver that provides more optimized or more relevant DNS answers and is accessible using Oblivious HTTP, and might want to advertise support for Oblivious HTTP via mechanisms like Discovery of Designated Resolvers ([DDR]) and Discovery of Network-designated Resolvers ([DNR]). Clients can access these gateways through trusted relays.

This document defines a way to use DNS resource records (RRs) to advertise that an HTTP service supports Oblivious HTTP. This advertisement is a parameter that can be included in SVCB and HTTPS DNS RRs [SVCB] (Section 4). The presence of this parameter indicates that a service can act as a target and has a gateway that can provide access to the target.

The client learns the URI to use for the gateway using a well-known URI suffix [WELLKNOWN], "ohttp-gateway", which is accessed on the target (Section 5). This means that for deployments that support this kind of discovery, the gateway and target resources need to be located on the same host.

This document also defines a way to fetch a gateway's key configuration from the gateway (Section 6).

This mechanism does not aid in the discovery of relays; relay configuration is out of scope for this document. Models in which this discovery mechanism is applicable are described in Section 3.

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. Applicability

There are multiple models in which the discovery mechanism defined in this document can be used.

* Upgrading regular (non-proxied) HTTP to Oblivious HTTP. In this model, the client intends to communicate with a specific target service, and prefers to use Oblivious HTTP if it is available. The target service has a gateway that it offers to allow access using Oblivious HTTP. Once the client learns about the gateway, it "upgrades" its requests from non-proxied HTTP to Oblivious HTTP to access the target service.

* Discovering alternative Oblivious HTTP services. In this model, the client has a default target service that it uses. For example, this may be a public DNS resolver that is accessible over Oblivious HTTP. The client is willing to use alternative target services if they are discovered, which may provide more optimized or more relevant responses.

In both deployment models, the client is configured with a relay that it trusts for Oblivious HTTP transactions. This relay either needs to provide generic access to gateways, or provide a service to clients to allow them to check which gateways are accessible.

4. The ohttp SvcParamKey

The "ohttp" SvcParamKey is used to indicate that a service described in an SVCB RR can be accessed as a target using an associated gateway. The service that is queried by the client hosts one or more target resources.

In order to access the service's target resources using Oblivious HTTP, the client needs to send encapsulated messages to the gateway resource and the gateway's key configuration (both of which can be retrieved using the method described in Section 6).

Both the presentation and wire format values for the "ohttp" parameter **MUST** be empty.

Services can include the "ohttp" parameter in the mandatory parameter list if the service is only accessible using Oblivious HTTP. Marking the "ohttp" parameter as mandatory will cause clients that do not understand the parameter to ignore that SVCB RR. Including the "ohttp" parameter without marking it mandatory advertises a service that is optionally available using Oblivious HTTP. Note also that multiple SVCB RRs can be provided to indicate separate configurations.

The media type to use for encapsulated requests made to a target service depends on the scheme of the SVCB RR. 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.

4.1. Use in HTTPS service RRs

For the "https" scheme, which uses the HTTPS RR type instead of SVCB, the presence of the "ohttp" parameter means that the target being described is an Oblivious HTTP service that is accessible using the default "message/bhttp" media type [OHTTP] [BINARY-HTTP].

For example, an HTTPS service RR for svc.example.com that supports Oblivious HTTP could look like this:

```
svc.example.com. 7200  IN HTTPS 1 . ( alpn=h2 ohttp )
```

A similar RR for a service that only supports Oblivious HTTP could look like this:

```
svc.example.com. 7200  IN HTTPS 1 . ( mandatory=ohttp ohttp )
```

4.2. Use in DNS server SVCB RRs

For the "dns" scheme, as defined in [DNS-SVCB], the presence of the "ohttp" parameter means that the DNS server being described has a DNS over HTTP (DoH) [DOH] service that can be accessed using Oblivious HTTP. Requests to the resolver are sent to the gateway using binary HTTP with the default "message/bhttp" media type [BINARY-HTTP], containing inner requests that use the "application/dns-message" media type [DOH].

If the "ohttp" parameter is included in an DNS server SVCB RR, the "alpn" **MUST** include at least one HTTP value (such as "h2" or "h3").

In order for DoH-capable recursive resolvers to function as Oblivious HTTP targets, their associated gateways need to be accessible via a client-trusted relay. DoH recursive resolvers used with the discovery mechanisms described in this section can either be publicly accessible, or specific to a network. In general, only publicly accessible DoH recursive resolvers will work as Oblivious HTTP targets, unless there is a coordinated deployment with a relay to access the network-specific DoH recursive resolvers.

4.2.1. Use with DDR

Clients can discover that a DoH recursive resolvers support Oblivious HTTP using DDR, either by querying _dns.resolver.arpa to a

locally configured resolver or by querying using the name of a resolver [DDR].

For example, a DoH service advertised over DDR can be annotated as supporting resolution via Oblivious HTTP using the following RR:

```
_dns.resolver.arpa  7200  IN SVCB 1 doh.example.net (
     alpn=h2 dohpath=/dns-query{?dns} ohttp )
```

Clients still need to perform verification of oblivious DoH servers, specifically the TLS certificate checks described in Section 4.2 of [DDR]. Since the gateway and target resources for discovered oblivious services need to be on the same host, this means that the client needs to verify that the certificate presented by the gateway passes the required checks. These checks can be performed when looking up the configuration on the gateway as described in Section 6, which can either be done directly or via the relay or another proxy to avoid exposing client IP addresses.

Opportunistic discovery [DDR], where only the IP address is validated, **SHOULD NOT** be used in general with Oblivious HTTP, since this mode primarily exists to support resolvers that use private or local IP addresses, which will usually not be accessible when using a relay. If a configuration occurs where the resolver is accessible, but cannot use certificate-based validation, the client **MUST** ensure that the relay only accesses the gateway and target using the unencrypted resolver's original IP address.

For the case of DoH recursive resolvers, clients also need to ensure that they are not being targeted with unique DoH paths that would reveal their identity. See Section 7 for more discussion.

4.2.2. 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 that learn about DoH recursive resolvers still need to ensure that they are not being targeted with unique DoH paths that would reveal their identity. See Section 7 for more discussion.

5. Gateway Location

Once a client has discovered that a service supports Oblivious HTTP via the "ohttp" parameter in a SVCB or HTTPS RR, it needs to be able to send requests via a relay to the correct gateway location.

This document defines a well-known resource ([WELLKNOWN]), "/.well-known/ohttp-gateway", which is an Oblivious Gateway Resource available on the same host as the target resource.

Some servers might not want to operate the gateway on a well-known URI. In such cases, these servers can use 3xx redirection responses (Section 15.4 of [HTTP]) to direct clients and relays to the correct location of the gateway. Such redirects would apply both to requests made to fetch key configurations (as defined in Section 6) and to encapsulated requests made via a relay.

If a client receives a redirect when fetching the key configuration from the well-known gateway resource, it **MUST NOT** communicate the redirected gateway URI to the relay as the location of the gateway to use. Doing so would allow the gateway to target clients by encoding unique or client-identifying values in the redirected URI. Instead, relays being used with dynamically discovered gateways **MUST** use the well-known gateway resource and follow any redirects independently of redirects that clients received. The relay can remember such redirects across oblivious requests for all clients in order to avoid added latency.

6. Key Configuration Fetching

Clients also need to know the key configuration of a gateway before encapsulating and sending requests to the relay.

If a client fetches the key configuration directly from the gateway, it will expose identifiers like a client IP address to the gateway. The privacy and security implications of fetching the key configuration are discussed more in Section 7. Clients can use an HTTP proxy to hide their IP addresses when fetching key configurations. Clients can also perform consistency checks to validate that they are not receiving unique key configurations, as discussed in Section 7.1.

In order to fetch the key configuration of a gateway discovered in the manner described in Section 5, the client issues a GET request (either through a proxy or directly) to the URI of the gateway specifying the "application/ohttp-keys" ([OHTTP]) media type in the Accept header.

For example, if the client knows an oblivious gateway URI, "https://svc.example.com/.well-known/ohttp-gateway", it could fetch the key configuration with the following request:

```
GET /.well-known/ohttp-gateway HTTP/1.1
Host: svc.example.com
Accept: application/ohttp-keys
```

Gateways that coordinate with targets that advertise Oblivious HTTP support **SHOULD** support GET requests for their key configuration in this manner, unless there is another out-of-band configuration model that is usable by clients. Gateways respond with their key configuration in the response body, with a content type of "application/ohttp-keys".

7. Security and Privacy Considerations

Attackers on a network can remove SVCB information from cleartext DNS answers that are not protected by DNSSEC [DNSSEC]. This can effectively downgrade clients. However, since SVCB indications for Oblivious HTTP support are just hints, a client can mitigate this by always checking for a gateway configuration (Section 6) on the well-known gateway location (Section 5). Use of encrypted DNS along with DNSSEC can also be used as a mitigation.

When clients fetch a gateway's configuration (Section 6), they can expose their identity in the form of an IP address if they do not connect via a proxy or some other IP-hiding mechanism. In some circumstances, this might not be a privacy concern, since revealing that a particular client IP address is preparing to use an Oblivious HTTP service can be expected. However, if a client is otherwise trying to hide its IP address or location (and not merely decouple its specific requests from its IP address), or if revealing its IP address facilitates key targeting attacks (if a gateway service uses IP addresses to associate specific configurations with specific clients), a proxy or similar mechanism can be used to fetch the gateway's configuration.

When discovering designated oblivious DoH recursive resolvers using this mechanism, clients need to ensure that the designation is trusted in lieu of being able to directly check the contents of the gateway server's TLS certificate. See Section 4.2.1 for more discussion, as well as the Security Considerations of [DNS-SVCB].

7.1. Key Targeting Attacks

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 targeting attacks. [CONSISTENCY] provides an overview of the options for ensuring the key configurations are consistent between different clients. Clients **SHOULD** employ some technique to mitigate key

targeting attacks, such as the option of confirming the key with a shared proxy as described in [CONSISTENCY]. If a client detects that a gateway is using per-client targeted key configuration, the client can stop using the gateway, and potentially report the targeting attack to let other clients avoid using this gateway in the future.

7.2. dohpath Targeting Attacks

For oblivious DoH servers, an attacker could use unique dohpath values to target or identify specific clients. This attack is very similar to the generic OHTTP key targeting attack described above.

A client can avoid these targeting attacks by only allowing a single dohpath value, such as the commonly used "/dns-query{?dns}" or another pre-known value. If the client allows arbitrary dohpath values, it **SHOULD** mitigate targeting attacks with a consistency check, such as using a mechanism described in [CONSISTENCY] to validate the dohpath value with another source. Clients might choose to only employ a consistency check on a percentage of discovery events, depending on the capacity of consistency check options and their deployment threat model.

8. IANA Considerations

8.1. SVCB Service Parameter

This document adds the following entry to the SVCB Service Parameters registry ([SVCB]). The definition of this parameter is in Section 4.

Number	Name	Meaning	Reference
8 (Early Allocation)	ohttp	Denotes that a service operates an Oblivious HTTP target	(This document)

Table 1

8.2. Well-Known URI

IANA is requested to add one new entry in the "Well-Known URIs" registry [WELLKNOWN].

URI suffix: ohttp-gateway

Change controller: IETF

Specification document: This document

Status: permanent

Related information: N/A

9. References

9.1. Normative References

[BINARY-HTTP] Thomson, M. and C. A. Wood, "Binary Representation of HTTP Messages", RFC 9292, DOI 10.17487/RFC9292, August 2022, <https://www.rfc-editor.org/rfc/rfc9292>.

[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-10, 5 August 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-add-ddr-10>.

[DNR] Boucadair, M., Reddy.K, 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-16, 27 April 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-add-dnr-16>.

[DNS-SVCB] Schwartz, B. M., "Service Binding Mapping for DNS Servers", Work in Progress, Internet-Draft, draft-ietf-add-svcb-dns-09, 26 June 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-add-svcb-dns-09>.

[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>.

[HTTP] Fielding, R., Ed., Nottingham, M., Ed., and J. Reschke, Ed., "HTTP Semantics", STD 97, RFC 9110, DOI 10.17487/RFC9110, June 2022, <https://www.rfc-editor.org/rfc/rfc9110>.

[OHTTP] Thomson, M. and C. A. Wood, "Oblivious HTTP", Work in Progress, Internet-Draft, draft-ietf-ohai-ohttp-10, 25 August 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-ohai-ohttp-10>.

[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. M., 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-12, 11 March 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-svcb-https-12>.

[WELLKNOWN] Nottingham, M., "Well-Known Uniform Resource Identifiers (URIs)", RFC 8615, DOI 10.17487/RFC8615, May 2019, <https://www.rfc-editor.org/rfc/rfc8615>.

9.2. Informative References

[CONSISTENCY] Davidson, A., Finkel, M., Thomson, M., and C. A. Wood, "Key Consistency and Discovery", Work in Progress, Internet-Draft, draft-ietf-privacypass-key-consistency-01, 10 July 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-privacypass-key-consistency-01>.

[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>.

Authors' Addresses

Tommy Pauly
Apple Inc.

Email: tpauly@apple.com

Tirumaleswar Reddy
Nokia

Email: kondtir@gmail.com