Workgroup:
Oblivious HTTP Application Intermediation
Internet-Draft: draft-ietf-ohai-svcb-config-00
Published: 24 October 2022
Intended Status: Standards Track
Expires: 27 April 2023
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/tfpauly/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 27 April 2023.

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 gates access to the target. The gateway is access 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 discover the client's identity.

Since Oblivious HTTP deployments will often involve very specific coordination between clients, relays, and gateways, the key configuration can often be shared in a bespoke fashion. However, some deployments involve clients discovering oblivious targets and their assoicated gateways 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 relays to access these gateways.

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

The client learns the URI to use for the oblivious gateway using a well-known URI [WELLKNOWN], "oblivious-gateway", which is accessed on the oblivious target (Section 5).

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

This mechanism does not aid in the discovery of oblivious 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 non-oblivious 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 an oblivious gateway that it offers to allow access using oblivious HTTP. Once the client learns about the oblivious gateway, it "upgrades" to using oblivious HTTP to access the target service.

* Discovering alternative oblivious HTTP services. In this model, the client has a default oblivious 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 oblivious target services if they are discovered, which may provide more optimized or more relevant responses.

In both of these deployment models, the client is assumed to already know of an oblivious relay that it trusts and works with. This oblivious relay either needs to provide generic access to oblivious gateways, or provide a service to clients to allow them to check which gateways are accessible.

4. The oblivious SvcParamKey

The "oblivious" SvcParamKey (Section 8) is used to indicate that a service described in an SVCB record can be accessed as an oblivious 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 obliviously, 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 "oblivious" parameter **MUST** be empty.

The "oblivious" parameter can be included in the mandatory parameter list to ensure that clients that do not support oblivious access do not try to use the service. Services that mark the oblivious parameter as mandatory can, therefore, indicate that the service might not be accessible in a non-oblivious fashion. Services that are intended to be accessed either obliviously or directly **SHOULD NOT** mark the "oblivious" parameter as mandatory. Note that since multiple SVCB responses can be provided for a single query, the oblivious and non-oblivious versions of a single service can have different SVCB records to support different names or properties.

The media type to use for encapsulated requests made to a target service 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.

4.1. Use in HTTPS service records

For the "https" scheme, which uses the HTTPS RR type instead of SVCB, the presence of the "oblivious" 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 record for svc.example.com that supports an oblivious gateway could look like this:

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

A similar record for a service that only support oblivious connectivity could look like this:

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

4.2. Use in DNS server SVCB records

For the "dns" scheme, as defined in [DNS-SVCB], the presence of the "oblivious" 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].

In order for DNS servers to function as oblivious targets, their associated gateways need to be accessible via an oblivious relay. Encrypted DNS servers used with the discovery mechanisms described in this section can either be publicly accessible, or specific to a network. In general, only publicly accessible DNS servers will work as oblivious DNS servers, unless there is a coordinated deployment with an oblivious relay that is also hosted within a network.

4.2.1. 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].

For example, a DoH service advertised over DDR can be annotated as supporting oblivious resolution using the following record:

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

Clients still need to perform some verification of oblivious DNS servers, such as the TLS certificate check described in [DDR]. This certificate check can be done 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.

For the case of DoH servers, 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 servers 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

Clients that know a service is available as an oblivious target via discovery through the "oblivious" parameter in a SVCB or HTTPS record need to know the location of the associated oblivious gateway before sending oblivious requests.

By default, the oblivious gateway for an oblivious target is defined as a well-known resource ([WELLKNOWN]) on the target, "/.well-known/oblivious-gateway".

Commonly, servers will not want to actually operate the oblivious gateway on a well-known URI. In such cases, servers can use 3xx redirection responses (Section 15.4 of [HTTP]) to direct clients and relays to the correct location of the oblivious gateway.

Generally, the first request a client will make will be a GET request to discover the key configuration, described in Section 6. This initial request also provides a convenient way for clients to learn about the redirect from the well-known resource, if there is a redirect. When clients work with their oblivious relays to send oblivious requests to the gateway, clients can communicate this redirected gateway URI.

6. Key Configuration Fetching

Clients also need to know the key configuration of an oblivious gateway before sending oblivious requests.

In order to fetch the key configuration of an oblivious gateway discovered in the manner described in Section 5, the client issues a GET request 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://osvc.example.com/gateway", it could fetch the key configuration with the following request:

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

Oblivious gateways that coordinate with targets that advertise oblivious 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".

Clients can either fetch this key configuration directly, or do so via a proxy in order to avoid the server discovering information about the client's identity. See Section 7 for more discussion of avoiding key targeting attacks.

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 support are just hints, a client can mitigate this by always checking for oblivious 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 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 gateway server's TLS certificate. See Section 4.2.1 for more discussion, as well as the Security Considerations of [SVCBDNS].

For oblivious DoH servers, an attacker could use unique DoH path values to target or identify specific clients. Clients can mitigate such attacks in several ways. Some options include: only allow common DoH paths (such as the de-facto default "/dns-query{?dns}"); performing consistency checks by fetching the information about the resolver over multiple resolution paths; or coordinating with a trusted oblivious relay to validate that DoH paths are common across clients using the same gateway.

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 analysis of the options for ensuring the key configurations are consistent between different clients. Clients **SHOULD** employ some technique to mitigate key targeting attack. Oblivious gateways that are detected to use targeted key configurations per-client **MUST NOT** be used.

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 obfuscate its IP address or location (and not merely decouple its specific requests from its IP address), or revealing its IP address will increase the risk of a key targeting attack (if a gateway service is trying to differentiate traffic across client IP addresses), a proxy or similar mechanism can be used to fetch the gateway's configuration.

8. IANA Considerations

8.1. SVCB Service Parameter

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

Number	Name	Meaning	Reference
TBD	oblivious	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: oblivious-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", Work in Progress, Internet-Draft, draft-ietf-httpbis-binary-message-06, 6 July 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-httpbis-binary-message-06>.

[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-13, 13 August 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-add-dnr-13>.

[DNS-SVCB] Schwartz, B. M., "Service Binding Mapping for DNS Servers", Work in Progress, Internet-Draft, draft-ietf-add-svcb-dns-07, 11 August 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-add-svcb-dns-07>.

[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-05, 26 September 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-ohai-ohttp-05>.

[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-11, 11 October 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-svcb-https-11>.

[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-wood-key-consistency-03, 17 August 2022, <https://datatracker.ietf.org/doc/html/draft-wood-key-consistency-03>.

[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>.

[SVCBDNS] Schwartz, B. M., "Service Binding Mapping for DNS Servers", Work in Progress, Internet-Draft, draft-ietf-add-svcb-dns-07, 11 August 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-add-svcb-dns-07>.

Authors' Addresses

Tommy Pauly
Apple Inc.

Email: tpauly@apple.com

Tirumaleswar Reddy
Nokia

Email: kondtir@gmail.com