Oblivious HTTP Application Intermediation
Internet-Draft
Intended status: Informational
Expires: 26 November 2022

T. Pauly
Apple Inc.
T. Reddy
Akamai

25 May 2022

Discovery of Oblivious Services via Service Binding Records
draft-pauly-ohai-svcb-config-01

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, as well as a mechanism to look up oblivious key configurations using a well-known URI.

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

Table of Contents

1. Introduction 2
2. Conventions and Definitions 3
3. The oblivious SvcParamKey 3
3.1. Use in HTTPS service records 4
3.2. Use in DNS server SVCB records 4
3.2.1. Use with DDR 4
3.2.2. Use with DNR 5
4. Configuration Well-Known URI 5
5. Security and Privacy Considerations 6
6. IANA Considerations 7
6.1. SVCB Service Parameter 7
6.2. Well-Known URI 7
7. References 7
7.1. Normative References 7
7.2. Informative References 8
Authors' Addresses 9

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 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]. The presence of this parameter indicates that a service has an oblivious target; see Section 3 of [OHTTP] for a description of oblivious targets.

This document also defines a well-known URI [RFC8615], "oblivious-configs", that can be used to look up key configurations on a service that is known to have an oblivious target.

This mechanism does not aid in the discovery of proxies to use to access oblivious targets; the configuration 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 oblivious SvcParamKey

The "oblivious" SvcParamKey Section 6 is used to indicate that a service described in an SVCB record can act as an oblivious target. Clients can issue requests to this service through an oblivious proxy once they learn the key configuration to use to encrypt messages to the oblivious target.

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 include mark oblivious support 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 as an oblivious target 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 scheme to use for oblivious requests made to a 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.

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

For example, an HTTPS service record for svc.example.com that supports an oblivious target could look like this:

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

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

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

3.2. 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, they need to be accessible via an oblivious proxy. 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 proxy that is also hosted within a network.

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].

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 resolver using the well-known URI (Section 4), which can either be done directly, or via a proxy to avoid exposing client IP addresses.

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.

4. Configuration Well-Known URI

Clients that know a service is available as an oblivious target, e.g., either via discovery through the "oblivious" parameter in a SVCB or HTTPS record, or by configuration, need to know the key configuration before sending oblivious requests.

This document defines a well-known URI [RFC8615], "oblivious-configs", that allows a target to host its configurations.

The URI is constructed using the TargetName in the associated ServiceMode SVCB record.

For example, the URI for the following record:

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

would be "https://svc.example.com/.well-known/oblivious-configs".

As another example, the URI for the following record:


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

would be "https://doh.example.net/.well-known/oblivious-configs".

The content of this resource is expected to be "application/ohttp-keys", as defined in [OHTTP].

Before being able to use a server as an oblivious target, clients need to use this URI to fetch the configuration. They can either fetch it directly, or do so via a proxy in order to avoid the server discovering information about the client's identity. See Section 5 for more discussion of avoiding key targeting attacks.

5. 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 target information. Use of encrypted DNS or DNSSEC also can be used as mitigations.

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 well as the Security Considerations of [I-D.ietf-add-svcb-dns].

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 targets that are detected to use targeted key configurations per-client MUST NOT be used.

When clients fetch a target's configuration using the well-known URI, they can expose their identity in the form of an IP addres if they do not connect via a proxy or some other IP-hiding mechanism. Clients SHOULD use a proxy or similar mechanism to avoid exposing client IPs to a target.

6. IANA Considerations

6.1. SVCB Service Parameter

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

Number	Name	Meaning	Reference
TBD	oblivious	Describes if a service has an oblivious target	(This document)

Table 1

6.2. Well-Known URI

IANA is requested to add a new entry in the "Well-Known URIs" registry [RFC8615] with the following information:

URI suffix: oblivious-configs

Change controller: IETF

Specification document: This document

Status: permanent

Related information: N/A

7. References

7.1. 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-04, 23 May 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-httpbis-binary-message-04>.

[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-06, 4 April 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-add-ddr-06>.

[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-07, 13 April 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-add-dnr-07>.

[DNS-SVCB] Schwartz, B., "Service Binding Mapping for DNS Servers", Work in Progress, Internet-Draft, draft-ietf-add-svcb-dns-03, 22 April 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-add-svcb-dns-03>.

[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>.

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

[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-10, 24 May 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-svcb-https-10>.

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>.

[I-D.ietf-add-svcb-dns]
Schwartz, B., "Service Binding Mapping for DNS Servers", Work in Progress, Internet-Draft, draft-ietf-add-svcb-dns-03, 22 April 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-add-svcb-dns-03>.

Authors' Addresses

Tommy Pauly
Apple Inc.
Email: tpauly@apple.com

Tirumaleswar Reddy
Akamai
Email: kondtir@gmail.com