DNS Privacy (dprive) Working Group
Internet-Draft
Intended status: Standards Track
Expires: July 5, 2018

S. Bortzmeyer
AFNIC

January 1, 2018

Encryption and authentication of the DNS resolver-to-authoritative communication
draft-bortzmeyer-dprive-resolver-to-auth-00

Abstract

This document proposes a mechanism for securing (privacy-wise) the communication between the DNS resolver and the authoritative name server.

REMOVE BEFORE PUBLICATION: this document should be discussed in the IETF DPRIVE group, through its mailing list. The source of the document, as well as a list of open issues, is currently kept at Github [1].

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 July 5, 2018.

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect

to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction and background

To improve the privacy of the DNS user ([RFC7626]), the standard solution is to encrypt the requests with TLS ([RFC7858]). We use this DNS-over-TLS solution as well here, since it is standardized, already implemented in many programs, and relies on a well-know security protocol (inventing a new security protocol is quite dangerous). But just encrypting, without authenticating the remote server, leaves the user's privacy vulnerable to active man-in-the-middle attacks. [RFC7858] and [I-D.ietf-dprive-dtls-and-tls-profiles] describe how to authenticate the DNS resolver, in the stub-to-resolver link. We describe here authentication of the authoritative name server, in the resolver-to-authoritative link.

A stub DNS resolver has only a few resolvers, and there is typically a pre-existing relationship. But a resolver speaks to many authoritative name servers, without any prior relationship. This means that, for instance, having a static key for the resolver makes sense while it would be clearly unrealistic for the authoritative server.

Instead, we rely on DANE ([RFC6698]). Authoritative name servers are known by name (obtained from zone delegation). The manager of the ns1.example.net name server adds a TLSA record under example.net. The client establishes the TLS session, then authentify in the normal DANE way.

The original charter of the DPRIVE working group, in force at the time of this draft, says "The primary focus of this Working Group is to develop mechanisms that provide confidentiality between DNS Clients and Iterative Resolvers" and adds "but it may also later consider mechanisms that provide confidentiality between Iterative Resolvers and Authoritative Servers". This document is here for this second step, "between Iterative Resolvers and Authoritative Servers". It will probably require a rechartering of the group.

2. Rules

A DNS full-service resolver who needs to query an authoritative name server establishes a TLS-over-TCP session with this authoritative name server. If the DNS material to perform DANE authentication is sent in the TLS session ([I-D.ietf-tls-dnssec-chain-extension]), it uses it. Otherwise, the resolver queries TLSA records ([RFC6698]) for this name server and authentifies the key or certificate of the server this way. If the name server is ns1.example.net, the TLSA record to query is _853._tcp.ns1.example.net.

Note that the server MAY use raw public keys ([RFC7250]) and so there is not always a certificate. If the server uses raw public keys, the TLSA record's Selector field must be 1 (SPKI, SubjectPublicKeyInfo).

The recommended order is to try TLS before querying the TLSA records. True, DANE signals if the server is willing to make DNS-over-TLS (and can therefore save a TLS attempt) but cannot guarantee that it will work (for instance if a middlebox blocks port 853). Also, the DANE records may be transferred in the TLS session, not through the DNS.

If the TLS session establishement fails, or if the DANE authentication fails, the result depends on whether the resolver runs in strict or opportunistic mode ([I-D.ietf-dprive-dtls-and-tls-profiles]). In strict mode, the resolver MUST stop using this authoritative name server, and MUST try other servers of the DNS zone. In opportunistic mode, the resolver MUST use the authoritative name server despite the failure. It MAY try other name servers of the zone before, in the hope they will accept TLS and be authentified. To avoid a chicken-and-egg problem, the resolver, even in strict mode, MAY use insecure servers for the meta-queries (getting the TLSA records). More specifically:

(0)The resolver remembers the keys of the authoritative name servers (in the same way it remembers the lowest RTT among a NS RRset),

(1)When the resolver needs to talk to a server (say ns2.example.net) for which it does not know the key, it does a TLSA request for _853._tcp.ns2.example.net,

(2)If the resolution of this request requires to talk to the very server we search the key for, the resolver connects to this server with TLS to port 853, does not bother to authenticate, and sends the query. This step offers no authentication.

(See also [I-D.ietf-dprive-dtls-and-tls-profiles], section 5.) A resolver MAY use the knowledge of TLS authentication it has to choose an authoritative name server among a NS RRset.

At the time of this document, it is expected that very few resolvers will use the strict mode, because there is not yet a deployment in authoritative name servers.

3. Operational considerations

DNS-over-TLS depends on TCP, and the resolver and the authoritative name server must therefore have persistent TCP connections ([RFC7766]).

A resolver may have a lot of client-side state, when managing hundreds of connections to remote authoritative servers ([tdns]).

The latency when connecting to a authoritative name server is certainly an issue. TLS 1.3 and TCP Fast Open ([RFC7413]) may help.

Open question: do we require a minimum TLS version of 1.3? ([I-D.ietf-tls-tls13])

Because the resolver cannot know in advance if the TLS connection will work (even if there is a DANE record), using parallel attemps ("happy eyeballs", [RFC8305]) is important. A resolver working in opportunistic mode should try port 53 and 853 in parallel.

An authoritative name server cannot know if the resolver authentified it, and how. In the future, it may be interesting to have a EDNS option to signal a successful authentication, or a failure, but this is out of scope currently.

If it is a concern that the same authoritative name servers are used for ordinary DNS and for encrypted DNS, there are several solutions. We may use front-end systems dispatching requests to port 53 and 853 to different servers.

A resolver must be configurable in mode strict or opportunistic (the strict mode is very unrealistic at this time and should not be the default). It may have a configuration to be in strict mode only for some domains.

4. IANA Considerations

No action for IANA. This section can be deleted.

5. Security Considerations

The state to be kept in both the client and the server may make some denial-of-service attacks easier. Following the advices of section 10 of [RFC7766] is recommended.

In opportunistic mode, there is no guarantee to have a secure use of the DNS, or even a guarantee to be informed of a problem. Opportunistic mode is a "best effort" privacy service. Even in strict mode, some leaks may occur, through the DANE meta-queries, and through SNI indication in the TLS session.

Encryption does not protect against a rogue server that will capture you requests and use them for evil purposes. It must therefore be combined with data minimization techniques ([RFC7816]).

6. References

6.1. Normative References

[I-D.ietf-dprive-dtls-and-tls-profiles]
Dickinson, S., Gillmor, D., and T. Reddy, "Usage and (D)TLS Profiles for DNS-over-(D)TLS", draft-ietf-dprive-dtls-and-tls-profiles-11 (work in progress), September 2017.

[RFC6698] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, DOI 10.17487/RFC6698, August 2012, <https://www.rfc-editor.org/info/rfc6698>.

[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>.

6.2. Informative References

[I-D.bortzmeyer-dprive-step-2]
Bortzmeyer, S., "Next step for DPRIVE: resolver-to-auth link", draft-bortzmeyer-dprive-step-2-05 (work in progress), December 2016.

[I-D.ietf-tls-dnssec-chain-extension]
Shore, M., Barnes, R., Huque, S., and W. Toorop, "A DANE Record and DNSSEC Authentication Chain Extension for TLS", draft-ietf-tls-dnssec-chain-extension-05 (work in progress), October 2017.

[I-D.ietf-tls-tls13]
Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", draft-ietf-tls-tls13-22 (work in progress), November 2017.

[RFC7250] Wouters, P., Ed., Tschofenig, H., Ed., Gilmore, J., Weiler, S., and T. Kivinen, "Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", RFC 7250, DOI 10.17487/RFC7250, June 2014, <https://www.rfc-editor.org/info/rfc7250>.

[RFC7413] Cheng, Y., Chu, J., Radhakrishnan, S., and A. Jain, "TCP Fast Open", RFC 7413, DOI 10.17487/RFC7413, December 2014, <https://www.rfc-editor.org/info/rfc7413>.

[RFC7626] Bortzmeyer, S., "DNS Privacy Considerations", RFC 7626, DOI 10.17487/RFC7626, August 2015, <https://www.rfc-editor.org/info/rfc7626>.

[RFC7766] Dickinson, J., Dickinson, S., Bellis, R., Mankin, A., and D. Wessels, "DNS Transport over TCP - Implementation Requirements", RFC 7766, DOI 10.17487/RFC7766, March 2016, <https://www.rfc-editor.org/info/rfc7766>.

[RFC7816] Bortzmeyer, S., "DNS Query Name Minimisation to Improve Privacy", RFC 7816, DOI 10.17487/RFC7816, March 2016, <https://www.rfc-editor.org/info/rfc7816>.

[RFC8305] Schinazi, D. and T. Pauly, "Happy Eyeballs Version 2: Better Connectivity Using Concurrency", RFC 8305, DOI 10.17487/RFC8305, December 2017, <https://www.rfc-editor.org/info/rfc8305>.

[tdns] Liang, Z., Wessels, D., Zi, H., Heidemann, J., Mankin, A., and N. Somaiya, "T-DNS: Connection-Oriented DNS to Improve Privacy and Security; USC/ISI Technical Report ISI-TR-706", August 2014, <http://www.isi.edu/~johnh/PAPERS/Zhu16b.pdf>.

6.3. URIs

[1] https://github.com/bortzmeyer/ietf-dprive-step-2

Appendix A. Acknowledgments

TODO

Appendix B. Alternatives

A comprehensive (?) list of other possible designs for this problem is in [I-D.bortzmeyer-dprive-step-2].

Author's Address

Stephane Bortzmeyer
AFNIC
1, rue Stephenson
Montigny-le-Bretonneux 78180
France

Phone: +33 1 39 30 83 46
Email: bortzmeyer+ietf@nic.fr
URI: http://www.afnic.fr/