dprive
Internet-Draft
Intended status: Standards Track
Expires: September 12, 2019

H. Zhang
P. Aras
Salesforce
W. Toorop
NLnet Labs
S. Dickinson
Sinodun IT
A. Mankin
Salesforce

March 11, 2019

DNS Zone Transfer over TLS
draft-hzpa-dprive-xfr-over-tls-01

Abstract

DNS zone transfers are transmitted in clear text, which gives attackers the opportunity to collect the content of a zone by eavesdropping on network connections. The DNS Transaction Signature (TSIG) mechanism is specified to restrict direct zone transfer to authorized clients only, but it does not add confidentiality. This document specifies use of DNS-over-TLS to prevent zone contents collection via passive monitoring of zone transfers.

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 http://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 September 12, 2019.

Table of Contents

1. Introduction

DNS has a number of privacy vulnerabilities, as discussed in detail in [I-D.bortzmeyer-dprive-rfc7626-bis]. Stub client to recursive resolver query privacy has received the most attention to date. There are now standards track documents for three encryption capabilities for stub to recursive queries and more work going on to guide deployment of specifically DNS-over-TLS (DoT) [RFC7858] and DNS-over-HTTPS (DoH) [RFC8484].

[I-D.bortzmeyer-dprive-rfc7626-bis] established that stub client DNS query transactions are not public and needed protection, but on zone transfer [RFC1995] [RFC5936] it says only:

"Privacy risks for the holder of a zone (the risk that someone gets the data) are discussed in [RFC5936] and [RFC5155]."

In what way is exposing the full contents of a zone a privacy risk? The contents of the zone could include information such as names of persons used in names of hosts. Best practice is not to use personal information for domain names, but many such domain names exist. There may also be regulatory, policy or other reasons why the zone contents in full must be treated as private.

Neither of the RFCs mentioned in [I-D.bortzmeyer-dprive-rfc7626-bis] contemplates the risk that someone gets the data through eavesdropping on network connections, only via enumeration or unauthorised transfer as described in the following paragraphs.

[RFC5155] specifies NSEC3 to prevent zone enumeration, which is when queries for the authenticated denial of existences records of DNSSEC allow a client to walk through the entire zone. Note that the need for this protection also motivates NSEC5 [I-D.vcelak-nsec5]; zone walking is now possible with NSEC3 due to crypto-breaking advances, and NSEC5 is a response to this problem.

[RFC5155] does not address data obtained outside zone enumeration (nor does [I-D.vcelak-nsec5]). Preventing eavesdropping of zone transfers (this draft) is orthogonal to preventing zone enumeration, though they aim to protect the same information.

[RFC5936] specifies using TSIG [RFC2845] for authorization of the clients of a zone transfer and for data integrity, but does not express any need for confidentiality, and TSIG does not offer encryption. Some operators use SSH tunnelling or IPSec to encrypt the transfer data.

Because the AXFR zone transfer is typically carried out over TCP from authoritative DNS protocol implementations, encrypting AXFR using DNS-over-TLS [RFC7858] seems like a simple step forward. This

document specifies how to use DoT to prevent zone collection from zone transfers, including discussion of approaches for IXFR, which uses UDP or TCP.

Next steps: Work on open questions at DNS table during IETF 104 Hackathon, expand this draft, then solicit discussion on the DPRIVE mailing list.

2. Terminology

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] and [RFC8174] when, and only when, they appear in all capitals, as shown here.

Privacy terminology is as described in Section 3 of [RFC6973].

DNS terminology is as described in [RFC8499].

DoT: DNS-over-TLS as specified in [RFC7858]

DoH: DNS-over-HTTPS as specified in [RFC8484]

3. Zone Transfer Confidentiality Overview

4. Zone Transfer with DoT - Authentication

4.1. TSIG

4.2. Mutual TLS

5. Session Establishment and Closing

5.1. AXFR Sessions

The connection flow in AXFR is a NOTIFY from the primary server to

the secondary server, and then an AXFR request from the secondary to the primary after which the data flows.

The connection for AXFR via DoT SHOULD be established using port 853, as specified in [RFC7858]. If there is no response on port 853, the connection MAY be attempted using port 443 in case the server offers DoT service on this port.

TODO: diagram of connection flow for AXFR, without and with DoT

5.2. IXFR Sessions

[RFC1995] specifies that Incremental Transfer may use UDP if the entire IXFR response can be contained in a single DNS packet, otherwise, TCP is used.

QUESTION: Given this, how should confidentiality of IXFR be provided?

To discuss:

- should IXFR have a mode in which TCP is mandatory?
- should IXFR have a mode in which TLS is mandatory?
- In workloads where there are frequent IXFRs, is the persistent connection mode that TCP-Mode would enable (as well as the retries) a benefit?

5.3. Policies for Both AXFR and IXFR

In order to assure the confidentiality of the zone information, entire group of servers involved in XFR (the primary and all secondaries) MUST have a consistent policy of requiring confidentiality. If any do not, this is a weak link for attackers to exploit. How to do this is TBD.

Additionally, the entire group of servers involved in XFR (the primary and all secondaries) MUST have a consistent policy of requiring Strict or Opportunistic DoT [RFC8310]. How to do this is TBD.

5.4. Next Steps

Upcoming IETF Hackathon experiments will feed into this Session Establishment and Closing section, as much about this needs exploration as well as discussion on the mailing list.

6. Performance Considerations

The details in [RFC7858] and [RFC8310] about e.g. using persistent connections and TLS Session Resumption [RFC5077] are fully applicable to DNS Zone Transfer over DoT as well.

7. Implementation Considerations

TBA

8. IANA Considerations

TBD

9. Security Considerations

This document specifies a security measure against a DNS risk: the risk that an attacker collects entire DNS zones through eavesdropping on clear text DNS zone transfers. It presents a new Security Consideration for DNS. Some questions to discuss are: should DoT in

this new case be required to use only TLS 1.3 and higher to avoid residual exposure? How should padding be used (if it should)?

10. Acknowledgements

The authors thank Benno Overeinder, Shumon Huque and Tim Wicinski for review and discussions.

11. Contributors

The following contributed significantly to the document:

12. Changelog

draft-hzpa-dprive-xfr-over-tls-01

- Editorial changes, updates to references.

draft-hzpa-dprive-xfr-over-tls-00

- Initial commit

13. Normative References

[I-D.bortzmeyer-dprive-rfc7626-bis]
Bortzmeyer, S. and S. Dickinson, "DNS Privacy Considerations", draft-bortzmeyer-dprive-rfc7626-bis-02 (work in progress), January 2019.

[I-D.vcelak-nsec5]
Vcelak, J., Goldberg, S., Papadopoulos, D., Huque, S., and D. Lawrence, "NSEC5, DNSSEC Authenticated Denial of Existence", draft-vcelak-nsec5-08 (work in progress), December 2018.

[RFC1995] Ohta, M., "Incremental Zone Transfer in DNS", RFC 1995, DOI 10.17487/RFC1995, August 1996, <https://www.rfc-editor.org/info/rfc1995>.

[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/info/rfc2119>.

[RFC2845] Vixie, P., Gudmundsson, O., Eastlake 3rd, D., and B. Wellington, "Secret Key Transaction Authentication for DNS (TSIG)", RFC 2845, DOI 10.17487/RFC2845, May 2000, <https://www.rfc-editor.org/info/rfc2845>.

[RFC5077] Salowey, J., Zhou, H., Eronen, P., and H. Tschofenig, "Transport Layer Security (TLS) Session Resumption without Server-Side State", RFC 5077, DOI 10.17487/RFC5077, January 2008, <https://www.rfc-editor.org/info/rfc5077>.

[RFC5155] Laurie, B., Sisson, G., Arends, R., and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", RFC 5155, DOI 10.17487/RFC5155, March 2008,

<https://www.rfc-editor.org/info/rfc5155>.

[RFC5936] Lewis, E. and A. Hoenes, Ed., "DNS Zone Transfer Protocol (AXFR)", RFC 5936, DOI 10.17487/RFC5936, June 2010, <https://www.rfc-editor.org/info/rfc5936>.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <https://www.rfc-editor.org/info/rfc6973>.

[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>.

[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/info/rfc8174>.

[RFC8310] Dickinson, S., Gillmor, D., and T. Reddy, "Usage Profiles for DNS over TLS and DNS over DTLS", RFC 8310, DOI 10.17487/RFC8310, March 2018, <https://www.rfc-editor.org/info/rfc8310>.

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

[RFC8499] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", BCP 219, RFC 8499, DOI 10.17487/RFC8499, January 2019, <https://www.rfc-editor.org/info/rfc8499>.

Authors' Addresses

Han Zhang

Salesforce
San Francisco, CA
United States

Email: hzhang@salesforce.com

Pallavi Aras
Salesforce
Herndon, VA
United States

Email: paras@salesforce.com

Willem Toorop
NLnet Labs
Science Park 400
Amsterdam 1098 XH
The Netherlands

Email: willem@nlnetlabs.nl

Sara Dickinson
Sinodun IT
Magdalen Centre
Oxford Science Park
Oxford OX4 4GA
United Kingdom

Email: sara@sinodun.com

Allison Mankin
Salesforce
Herndon, VA
United States

Email: allison.mankin@gmail.com