Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 28, 2020

A. Ghedini
Cloudflare, Inc.

February 25, 2020

Using Early Data in DNS over TLS
draft-ghedini-dprive-early-data-02

Abstract

This document illustrates the risks of using TLS 1.3 early data with DNS over TLS, and specifies behaviors that can be adopted by clients and servers to reduce those risks.

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 August 28, 2020.

Table of Contents

1. Introduction

TLS 1.3 [TLS13] defines a mechanism, called 0-RTT session resumption or early data, that allows clients to send data to servers in the first round-trip of a resumed connection without having to wait for the TLS handshake to complete.

This can be used to send DNS queries to DNS over TLS [DOT] servers without incurring in the cost of the additional round-trip required by the TLS handshake. This can provide significant performance improvements in cases where new DNS over TLS connections need to be established often such as on mobile clients where the network might not be stable, or on resolvers where keeping an open connection to many authoritative servers might not be practical.

However the use of early data allows an attacker to capture and replay the encrypted DNS queries carried on the TLS connection. This can have unwanted consequences and help in recovering information about those queries. While [TLS13] describes tecniques to reduce the likelihood of a replay attack, they are not perfect and still leave some potential for exploitation.

2. Notational Conventions

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. Early Data in DNS over TLS

Early data forms a single stream of data along with other application data, meaning that one or more DNS queries can either be partially or fully contained within early data. Once the TLS handshake has completed, the early data is known to not be a replayed copy of that data, but this doesn't mean that it can't be replayed, or that it hasn't already been replayed, in another connection.

A server can signal to clients whether it is willing to accept early data in future connections by providing the "early_data" TLS extension as part of a TLS session ticket, as well as limit the amount of early data it is willing to accept using the "max_early_data_size" field of the "early_data" extension.

In addition to the mitigation mechanisms mandated in [TLS13] that reduce the ability of an attacker to replay early data, but may not completely eliminate it, a server that decided to offer early data to clients MAY reject early data at the TLS layer, or delay the processing of early data after the handshake is completed.

If the server rejects early data at the TLS layer, a client MUST forget information it optmisitically assumed about the onnection when sending early data, such as the negotiated protocol [ALPN]. Any DNS queries sent in early data will need to be sent again, unless the client decides to abandon them.

Not all types of DNS messages are safe to be sent as early data, as they might modfify the server's state, or expose sensitive data, through replay. Clients MUST NOT use early data to send messages that make use of opcodes other than "Query" and RR types not listed in the registry defined in Section 5.1. Servers receiving any of those messages MUST reply with a "FormErr" response code.

4. Security Considerations

4.1. Information Exposure

By replaying DNS queries that were captured when transmitted over early data, an attacker might be able to expose information about those queries, even if encrypted.

For example, it's a common behavior for DNS servers to statefully rotate the order of RRs when replying to DNS queries for an RRSet that contains multiple RRs. If the order of rotation is predictable, replaying a captured early data DNS query and observing the order of RRs in DNS responses before and after the replayed query, might allow

the attacker to confirm whether the query targeted a specific name that was suspected of being queried.

When accepting early data, servers SHOULD either use fixed ordering for multiple RRs in the same DNS response or shuffle the RRs at random, but MUST NOT use stateful and deterministic ordering across multiple queries.

4.2. Denial of Service

Accepting early data exposes a server to potential denial of service through the replay of queries that might be expensive to handle.

When under load, a server MAY reject TLS early data such that the client is forced to retry them after the handshake is completed.

5. IANA Considerations

This document has no actions for IANA.

5.1. Registry for DNS Resource Record (RR) TYPEs for TLS Early Data

This document establishes a registry of DNS RR types that can be used within TLS early data, titled "DNS Resource Record (RR) TYPEs for Use with TLS Early Data", under the existing "Domain Name System (DNS) Parameters" heading.

The entries in the registry are:

TYPE	Reference
A	[this document]
NS	[this document]
CNAME	[this document]
SOA	[this document]
PTR	[this document]
MX	[this document]
TXT	[this document]
AAAA	[this document]
SRV	[this document]
DNAME	[this document]

DS	[this document]	
DNSKEY	[this document]	

The values in this registry MUST correspond to existing entries in the "Resource Record (RR) TYPEs" registry. Specifically, the value of the "TYPE" column for each entry in this new registry MUST match the value of the "TYPE" column of an entry in the "Resource Record (RR) TYPEs" registry.

6. References

6.1. Normative References

[DOT] 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>.

[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>.

[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>.

[TLS13] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

6.2. Informative References

[ALPN] Friedl, S., Popov, A., Langley, A., and E. Stephan, "Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension", RFC 7301, DOI 10.17487/RFC7301, July 2014, <https://www.rfc-editor.org/info/rfc7301>.

[RFC8470] Thomson, M., Nottingham, M., and W. Tarreau, "Using Early Data in HTTP", RFC 8470, DOI 10.17487/RFC8470, September 2018, <https://www.rfc-editor.org/info/rfc8470>.

Appendix A. Acknowledgments

Thanks to Martin Thomson, Mark Nottingham and Willy Tarreau for writing [RFC8470] which heavily inspired this document, and to Daniel Kahn Gillmor and Colm MacCarthaigh who also provided important ideas and contributions.

Author's Address

Alessandro Ghedini
Cloudflare, Inc.

Email: alessandro@cloudflare.com