Workgroup: TLS Working Group
Internet-Draft:
draft-pismenny-tls-dtls-plaintext-sequence-number-00
Published: 23 February 2023
Intended Status: Standards Track
Expires: 27 August 2023
Authors: B. Pismenny
NVIDIA

Plaintext Sequence Numbers for Datagram Transport Security Layer 1.3

Abstract

This document specifies a TLS 1.3 extension that enables DTLS 1.3 to negotiate the use of plaintext sequence numbers instead of protected sequence numbers. Plaintext sequence numbers are advantageous in closed networks where the benefits of lower latency outweigh the risk of ossification and reduced privacy.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Datagram Transport Layer Security (DTLS) 1.3 [RFC9147] packet encryption protects not only record data, but also the record header's sequence number. The sequence number is encrypted by XORing it with a mask which is generated by encrypting the leading 16 bytes of the record's ciphertext with a sequence number key.

For high performance networking, sequence number encryption is a trade-off between ossification and privacy on the one hand and latency and complexity for hardware acceleration on the other hand. Sequence number encryption improves privacy by hiding the real ordering of packets from on-path observers. Sequence number encryption also prevents protocol ossification, when middleboxes manipulate packet delivery based on the sequence number. Sequence number encryption however adds latency to packet processing on both sender and receiver. Sequence number encryption also increases the complexity and cost of NIC encryption accelerators, which are crucial for enabling encryption in high performance computing systems that seek to maximize performance and lowest penalty possible for encryption.

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. Sequence Number Encryption Extension

```
enum {
  default_cipher (0),
  plaintext (1),
  (65536)
} SeqNumEncAlgs;

struct {
  select (Handshake.msg_type) {
    case CH:
      SeqNumEncAlgs supported_algs<1..255>;

    case SH:
      SeqNumEncAlgs selected_alg;
  };
} SupportedSequenceNumberEncryptionAlgorithms;
```

> OPEN: This extension might fit nicely with the TLS flags extension [I-D.draft-ietf-tls-tlsflags], but TLS flags doesn't seem to apply to DTLS.

The "sequence_number_encryption_algorithms" extension is used by the client to specify the record sequence number encryption algorithms it supports and by the server to select the algorithm it prefers. The ClientHello message lists algorithms by the order of their preference, starting from the most preferred algorithm.

If this extension is not present, in either ClientHello or EncryptedExtensions, then both parties **MUST** fallback to the default record sequence number encryption algorithm.

> OPEN: Do we want an encrypted extension for the server's response? It is possible to use an encrypted extension, by using the default record sequence encryption algorithm prior to epoch 3 (epoch < 3), and enabling the selected algorithm only after epoch 3 (epoch >= 3).

4. Security Considerations

This document allows endpoints to disable the record sequence number encryption algorithm, which retracts the on-path tracking anti-ossification protection established in [RFC9147] record sequence number encryption. It is therefore **RECOMMENDED** that users limit the deployment of this extension to closed environments, such as data centers, where the risk of on-path observers is negligible.

5. IANA Considerations

IANA is requested to assign a new value from the TLS ExtensionType values registry:

- *The Extension Name should be sequence_number_encryption_algorithms
- *The TLS 1.3 value should be CH,HRR,SH
- *The DTLS-Only value should be Y
- *The Recommended value should be N
- *The Reference should be this document

6. Normative References

[I-D.draft-ietf-tls-tlsflags] Nir, Y., "A Flags Extension for TLS 1.3", Work in Progress, Internet-Draft, draft-ietf-tls-tlsflags-11, 27 January 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-tlsflags-11>.

[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>.

[RFC9147] Rescorla, E., Tschofenig, H., and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", RFC 9147, DOI 10.17487/RFC9147, April 2022, <https://www.rfc-editor.org/rfc/rfc9147>.

Acknowledgments

TODO acknowledge.

Author's Address

Boris Pismenny
NVIDIA

Email: boris.pismenny@gmail.com