Network Working Group
Internet-Draft
Intended status: Experimental
Expires: 14 November 2025

S. M. K. Varigonda
Samsung R&D Bangalore
R. S. R. Sige
Spirent

13 May 2025

Precision Time Protocol (PTP) Authentication Extension
draft-kumarvarigonda-ptp-auth-extension-00

Abstract

Precision Time Protocol (PTP), as defined in IEEE 1588-2019, lacks cryptographic security mechanisms, exposing deployments to message spoofing, delay attacks, and timestamp manipulation. This document defines an optional Authentication TLV (AUTH_TLV) using modern Authenticated Encryption with Associated Data (AEAD) algorithms to ensure message integrity,authenticity, and replay protection. It also provides example configurations, implementation approaches, and test strategies.

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 14 November 2025.

Copyright Notice

Table of Contents

1. Introduction

The PTP protocol is widely used for time synchronization in telecom, industrial automation, and financial systems. However, the protocol lacks built-in security. This draft proposes a lightweight extension for cryptographic message authentication and integrity without impacting compatibility.

2. Problem Statement

PTP messages are susceptible to:

* Spoofing of SYNC or ANNOUNCE messages

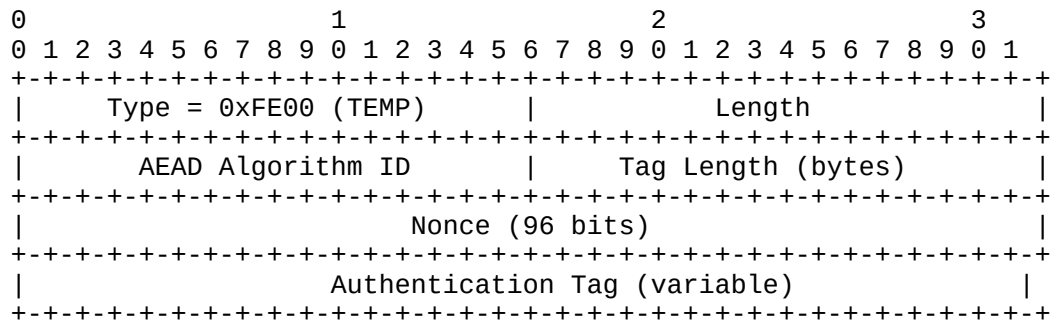
* Timestamp alteration during transit

* Replay or delay injection attacks

These vulnerabilities can compromise distributed systems relying on synchronized time for control, logs, or access control.

3. AUTH TLV Format

A new TLV is introduced as follows:



The nonce is derived from the message sequence ID and clock ID.

Supported AEAD algorithms:

* AES-GCM-128/256 (ID 0x0001)

* ChaCha20-Poly1305 (ID 0x0002)

4. AEAD Algorithm Support

The AUTH TLV uses AEAD for combined encryption and authentication, though only authentication is used in this extension. The message body is used as AAD, and only the tag is appended in the TLV.

5. Key Management

Keys may be provisioned using:

* Manual configuration (secure local access)

* Enrollment via PKI (e.g., EST, SCEP)

* TPM-based secure provisioning (future work)

6. Backward Compatibility

As per IEEE 1588 TLV rules, unknown TLVs are ignored by legacy systems. Authentication failures are not enforced unless explicitly configured.

7. Example Implementations

7.1. Software (ptp4l)

Modify ptp4l to:

* Enable auth_tlv_enable = 1 in configuration

* Parse and verify AUTH TLV using OpenSSL or libsodium

* Generate tag for outgoing messages with unique nonce

7.2. Hardware

Suggested flow for hardware timestamping with AUTH:

* Timestamp before encryption

* Use on-NIC AEAD (if supported) or offload via driver extensions

* Expose configuration via ethtool or netlink extensions

7.3. Wireshark Filters

Use the following filter:

ptp.messageType && frame contains 0xfe00

Custom dissector patches can be developed to interpret the AUTH_TLV fields.

8. Security Considerations

- Nonce reuse must be avoided; use a deterministic counter with a unique base per node. - Replay attacks are mitigated by validating sequence IDs and time windows. - Integrity is ensured only for messages using AUTH TLV.

9. IANA Considerations

Request registration of:

* AUTH_TLV type code (tentatively 0xFE00 for testing)

* AEAD Algorithm ID registry for PTP

10. Appendix A. Sample ptp4l.conf

```
[global]
auth_tlv_enable 1
auth_algorithm 2
auth_key 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
auth_nonce_base 112233445566778899aabb
auth_tag_len 16
auth_debug 1
```

11. Appendix B. Example AUTH TLV

```
   TLV Type: 0xFE00
   Length:   32
   AEAD ID:  0x0002
   Tag Len:  16
   Nonce:    00 11 22 33 44 55 66 77 88 99 aa bb
   Tag:      c0 ff ee 12 34 56 78 90 de ad be ef 12 34 56 78
```

12. Appendix C: Change Log

draft-kumarvarigonda-ospf-precomputed-frr-00

- Initial version including use case, diagram, and examples.

Authors' Addresses

Srinivasa Mohan Kumar Varigonda
Samsung R&D Bangalore
Email: sri.mohan@samsung.com

Rama Subba Reddy Sige
Spirent
Email: rama.subbareddy@spirent.com