opsawg
Internet-Draft
Intended status: Standards Track
Expires: 16 November 2026

X. Gao, Ed.
S. Zhang
China Unicom
C. Lin
New H3C Technologies

15 May 2026

Export of TLS Handshake Information in IPFIX
draft-gao-opsawg-ipfix-term-and-app-02

Abstract

This document defines a set of new Information Elements (IEs) in the IPFIX Information Model for exporting raw TLS ClientHello handshake fields. These IEs enable the collection of standardized client behavioral fingerprints from network traffic without decryption of the encrypted payload. The exported fields facilitate network anomaly detection, threat identification, and fault diagnosis in encrypted traffic environments.

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 16 November 2026.

Copyright Notice

Table of Contents

1. Introduction

As encrypted transmission via TLS has become ubiquitous across all network traffic, the payload content of business communications is no longer visible. The plaintext TLS ClientHello handshake fields have emerged as one of the few stable and exploitable analysis entry points in encrypted traffic. Various types of malware, remote access trojans (RATs), ransomware, and DDoS attack tools all carry distinctive TLS client fingerprints, which serve as core identifiers for threat detection, attribution analysis, and forensic investigation in encrypted traffic scenarios. Telecommunications operators, cloud service providers, and enterprise networks, when performing security operations such as anomaly detection, crawler identification, and attack attribution, urgently require standardized, interoperable, and comparable client fingerprinting features derived from the plaintext TLS ClientHello fields.

Currently, TLS client fingerprint field export in the industry is predominantly implemented through proprietary vendor-specific solutions, which suffer from inconsistent data formats, divergent collection rules, and inability to perform collaborative parsing across devices. To address these issues, it is necessary to define standardized specifications for core fingerprint fields within the

IPFIX information model, so as to achieve unified collection, standardized export, universal parsing, and cross-domain comparison of fingerprinting features, thereby enhancing the compatibility and scalability of end-to-end security operations and situational awareness systems.

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. Sample Use Cases

3.1. Problem Description

Endpoints within home broadband networks, such as computers, smartphones, surveillance cameras, and routers, may, due to malware infection, firmware vulnerabilities, or unauthorized access, proactively initiate TLS connections to external suspicious servers without the user’s awareness. Such connections are typically employed for malware command and control, network scanning, or crawler access, representing a typical form of anomalous outbound traffic. Due to TLS encryption, traditional traffic analysis methods are unable to identify client fingerprinting features. The majority of malware, remote access tools, and crawler scripts utilize lightweight TLS libraries, whose handshake characteristics differ significantly from standard browsers. By evaluating TLS handshake characteristics, it becomes possible to determine whether a connection originates from an anomalous client, thereby enabling precise detection and remediation.

3.2. Solution

By deploying IPFIX-based traffic collection and analysis capabilities on critical network gateways and boundary devices such as telecom operator residential broadband BRAS (Broadband Remote Access Server), cloud gateways, enterprise egress routers, and backbone network monitoring points, the system extracts key TLS client fingerprint characteristic fields losslessly from TLS handshake packets. This enables feature export and centralized reporting without traffic decryption. Through traffic collection and analysis platforms, fingerprint modeling, whitelist comparison, and anomalous feature analysis are performed, thereby achieving behavior identification and operational closed-loop remediation for encrypted traffic anomalous outbound connections, malware, remote access tools, crawlers, and

similar threats.

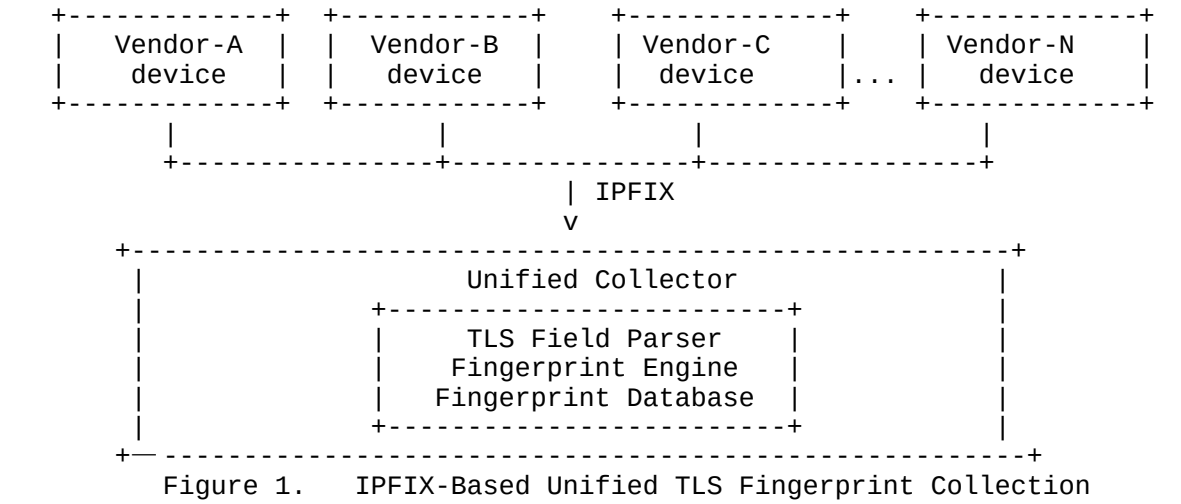

Figure 1. IPFIX-Based Unified TLS Fingerprint Collection

The TLS field parser is responsible for parsing and extracting key TLS handshake field information from IPFIX exported elements. The fingerprint engine performs the modeling and construction of client fingerprints based on raw TLS handshake field data collected via IPFIX. The characteristic fingerprint database is a database used for the standardized storage of various known and identifiable feature sets, the system performs real-time comparison and matching of the collected and generated client fingerprints against the characteristic fingerprint database.

4. New Information Elements

4.1. tlsClientHelloSNI

ElementID: TBD

Name: tlsClientHelloSNI

Abstract Data Type: string

Data Type Semantics: identifier

Description：The value of the Server Name Indication (SNI) extension in the TLS ClientHello message, which specifies the target server hostname (encoded in UTF - 8) as defined in Section 3 of RFC 6066 and used for certificate selection in multi - domain hosting scenarios.The Server Name Indication (SNI) extension enables a TLS client to indicate the name of the server it is attempting to connect to.This mechanism facilitates secure connections to servers hosting multiple virtual servers on a single network address.

Reference：See RFC 6066 section 3 for the specification of Server Name Indication.

4.2. tlsClientHelloVersion

ElementID: TBD

Name: tlsClientHelloVersion

Abstract Data Type: unsigned16

Data Type Semantics: identifier

Description：The TLS protocol version number negotiated during the handshake and used in the TLS record layer header, encoded as a 2-byte unsigned integer (e.g., 0x0304 for TLS 1.3) as defined in RFC 8446 and RFC 5246.

Reference：RFC 8446,RFC 5246

4.3. tlsClientHelloCipherSuite

ElementID: TBD

Name: tlsClientHelloCipherSuite

Abstract Data Type: unsigned16

Data Type Semantics: identifier

Description：A list of cipher suite values (each 2-byte unsigned integer) advertised by the client in the TLS ClientHello message.

Reference：RFC 8446

4.4. tlsClientHelloSSLExtension

ElementID: TBD

Name: tlsClientHelloSSLExtension

Abstract Data Type: unsigned16

Data Type Semantics: identifier

Description：A list of TLS extension type codes (each 2-byte unsigned integer) from the ClientHello extensions field.

Reference：RFC 8446

4.5. tlsClientHelloEllipticCurve

ElementID: TBD

Name:tlsClientHelloEllipticCurve

Abstract Data Type: unsigned16

Data Type Semantics: identifier

Description：A list of elliptic curve identifiers (each 2-byte unsigned integer) from the "elliptic_curves" extension in ClientHello.

Reference：RFC 8446

4.6. tlsClientHelloEllipticCurvePointFormat

ElementID: TBD

Name: tlsClientHelloEllipticCurvePointFormat

Abstract Data Type: unsigned16

Data Type Semantics: identifier

Description：A list of elliptic curve point format identifiers (each 1-byte unsigned integer) from the "elliptic_curves_point_formats" extension in ClientHello.

Reference：RFC 8446

5. Security Considerations

5.1. Privacy and Sensitive Information Risks

All fields defined in this document do not carry or process any user-sensitive information. They solely represent client software implementation characteristics and TLS cipher suite configuration features, and cannot independently be used to identify natural persons. These fingerprints are not uniquely bound to specific users, do not constitute personally identifiable information, and are not used for scenarios such as user behavior analysis or individual user identification. This mechanism solely achieves network anomalous traffic identification through fingerprint feature comparison, and does not introduce any risk of privacy leakage.

5.2. No Involvement of Traffic Decryption Operations

All exportable metadata fields specified in this document are solely derived from the TLS plaintext handshake phase. The data collection and processing workflow of this solution does not perform decryption, parsing, or storage of user encrypted communications. Only publicly available handshake metadata is collected, without accessing the user-encrypted business data in transit. Such transport layer behavioral characteristics have abundant mature application precedents in the IETF standards ecosystem, and are consistent with the application paradigm of traditional transport layer metadata mechanisms such as TCP options.

5.3. Risk Control Against Misuse

To prevent improper use or malicious abuse of the TLS fingerprint fields defined in this document, the following constraints and principles shall be strictly observed during the deployment and application of this mechanism:

Legitimate use restrictions: This mechanism shall only be used for compliant network management scenarios, including but not limited to network operations, anomalous traffic detection, network fault troubleshooting, DDoS attack mitigation, and other legitimate business purposes.

Prohibition of non-compliant use: This mechanism shall be strictly prohibited from being used in unauthorized, non-network-management scenarios such as cross-domain user tracking, user profiling, or individual behavior monitoring.

Transmission access control: For TLS fingerprint data transmission based on the IPFIX protocol, communication privileges between collectors and exporters shall be restricted through mechanisms such as Access Control Lists (ACL) and authentication, so as to ensure transmission security.

Data minimization: All collected traffic feature data shall strictly adhere to the data minimization principle. Long-term storage of redundant or irrelevant traffic feature data is prohibited, so as to minimize potential security risks.

6. IANA Considerations

The document makes a request to IANA to register the Information Elements defined in section 4.

Authors' Addresses

Xing Gao (editor)
China Unicom
Beijing
China
Email: gaox60@chinaunicom.cn

Shuai Zhang
China Unicom
Beijing
China
Email: zhangs366@chinaunicom.cn

Changwang Lin
New H3C Technologies
Beijing
China
Email: linchangwang.04414@h3c.com