Internet Engineering Task Force (IETF)
Request for Comments: 8460
Category: Standards Track
ISSN: 2070-1721

D. Margolis
Google, Inc.
A. Brotman
Comcast, Inc.
B. Ramakrishnan
Oath, Inc.
J. Jones
Microsoft, Inc.
M. Risher
Google, Inc.

September 2018

SMTP TLS Reporting

Abstract

A number of protocols exist for establishing encrypted channels between SMTP Mail Transfer Agents (MTAs), including STARTTLS, DNS-Based Authentication of Named Entities (DANE) TLSA, and MTA Strict Transport Security (MTA-STS). These protocols can fail due to misconfiguration or active attack, leading to undelivered messages or delivery over unencrypted or unauthenticated channels. This document describes a reporting mechanism and format by which sending systems can share statistics and specific information about potential failures with recipient domains. Recipient domains can then use this information to both detect potential attacks and diagnose unintentional misconfigurations.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The STARTTLS extension to SMTP [RFC3207] allows SMTP clients and hosts to establish secure SMTP sessions over TLS. The protocol design uses an approach that has come to be known as "Opportunistic Security" (OS) [RFC7435]. This method maintains interoperability with clients that do not support STARTTLS, but it means that any attacker could potentially eavesdrop on a session. An attacker could perform a downgrade or interception attack by deleting parts of the SMTP session (such as the "250 STARTTLS" response) or redirect the entire SMTP session (perhaps by overwriting the resolved MX record of the delivery domain).

Because such "downgrade attacks" are not necessarily apparent to the receiving MTA, this document defines a mechanism for sending domains to report on failures at multiple stages of the MTA-to-MTA conversation.

Recipient domains may also use the mechanisms defined by MTA-STS [RFC8461] or DANE [RFC6698] to publish additional encryption and authentication requirements; this document defines a mechanism for sending domains that are compatible with MTA-STS or DANE to share success and failure statistics with recipient domains.

Specifically, this document defines a reporting schema that covers failures in routing, DNS resolution, and STARTTLS negotiation; policy validation errors for both DANE [RFC6698] and MTA-STS [RFC8461]; and a standard TXT record that recipient domains can use to indicate where reports in this format should be sent. The report can also serve as a heartbeat to indicate that systems are successfully negotiating TLS during sessions as expected.

This document is intended as a companion to the specification for SMTP MTA-STS [RFC8461] and adds reporting abilities for those implementing DANE [RFC7672].

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

We also define the following terms for further use in this document:

- MTA-STS Policy: A mechanism by which administrators can specify the expected TLS availability, presented identity, and desired actions for a given email recipient domain. MTA-STS is defined in [RFC8461].

- DANE Policy: A mechanism by which administrators can use DNSSEC to commit an MTA to support STARTTLS and to publish criteria to be used to validate its presented certificates. DANE for SMTP is defined in [RFC7672], with the base specification defined in [RFC6698] (and updated by [RFC7671]).

- TLSRPT (TLS Reporting) Policy: A policy specifying the endpoint to which Sending MTAs should deliver reports.

- Policy Domain: The domain against which a TLSRPT, an MTA-STS, or a DANE policy is defined. For TLSRPT and MTA-STS, this is typically the same as the envelope recipient domain [RFC5321], but when mail is routed to a "smarthost" gateway by local policy, the "smarthost" domain name is used instead. For DANE, the Policy Domain is the "TLSA base domain" of the receiving SMTP server as described in Section 2.2.3 of RFC 7672 and Section 3 of RFC 6698.

- Sending MTA: The MTA initiating the relay of an email message.

- Aggregate Report URI (rua): A comma-separated list of locations where the report is to be submitted.

- ABNF: Augmented Backus-Naur Form, a syntax for formally specifying syntax, defined in [RFC5234] and [RFC7405].

2. Related Technologies

- This document is intended as a companion to the specification for SMTP MTA-STS [RFC8461].

- SMTP TLSRPT defines a mechanism for sending domains that are compatible with MTA-STS or DANE to share success and failure statistics with recipient domains. DANE is defined in [RFC6698], and MTA-STS is defined in [RFC8461].

3. Reporting Policy

A domain publishes a record to its DNS indicating that it wishes to receive reports. These SMTP TLSRPT policies are distributed via DNS from the Policy Domain's zone as TXT records (similar to Domain-based Message Authentication, Reporting, and Conformance (DMARC) policies) under the name "_smtp._tls". For example, for the Policy Domain "example.com", the recipient's TLSRPT policy can be retrieved from "_smtp._tls.example.com".

Policies consist of the following directives:

- "v": This document defines version 1 of TLSRPT, for which this value MUST be equal to "TLSRPTv1". Other versions may be defined in later documents.

- "rua": A URI specifying the endpoint to which aggregate information about policy validation results should be sent (see Section 4, "Reporting Schema", for more information). Two URI schemes are supported: "mailto" and "https". As with DMARC [RFC7489], the Policy Domain can specify a comma-separated list of URIs.

- In the case of "https", reports should be submitted via POST [RFC7231] to the specified URI. Report submitters MAY ignore certificate validation errors when submitting reports via HTTPS POST.

- In the case of "mailto", reports should be submitted to the specified email address [RFC6068]. When sending failure reports via SMTP, Sending MTAs MUST deliver reports despite any TLS-related failures and SHOULD NOT include this SMTP session in the next report. This may mean that the reports are delivered unencrypted. Reports sent via SMTP MUST contain a valid DomainKeys Identified Mail (DKIM) [RFC6376] signature by the reporting domain. Reports lacking such a signature MUST be ignored by the recipient. DKIM signatures MUST NOT use the "l=" attribute to limit the body length used in the signature. This ensures attackers cannot append extraneous or misleading data to a report without breaking the signature. The DKIM TXT record SHOULD contain the appropriate service type declaration, "s=tlsrpt". If not present, the receiving system MAY ignore reports lacking that service type.

Sample DKIM record:

```
dkim_selector._domainkey.example.com TXT
      "v=DKIM1;k=rsa;s=tlsrpt;p=Mlf4qwSZfase4fa=="
```

The formal definition of the "_smtp._tls" TXT record, defined using [RFC5234] and [RFC7405], is as follows:

```
tlsrpt-record     = tlsrpt-version 1*(field-delim tlsrpt-field)
                    [field-delim]

field-delim       = *WSP ";" *WSP

tlsrpt-field      = tlsrpt-rua /        ; Note that the
                    tlsrpt-extension    ; tlsrpt-rua record is
                                        ; required.

tlsrpt-version    = %s"v=TLSRPTv1"

tlsrpt-rua        = %s"rua="
                    tlsrpt-uri *(*WSP "," *WSP tlsrpt-uri)

tlsrpt-uri        = URI
                    ; "URI" is imported from [RFC3986];
                    ; commas (ASCII 0x2C), exclamation
                    ; points (ASCII 0x21), and semicolons
                    ; (ASCII 0x3B) MUST be encoded

tlsrpt-extension  = tlsrpt-ext-name "=" tlsrpt-ext-value

tlsrpt-ext-name   = (ALPHA / DIGIT) *31(ALPHA /
                    DIGIT / "_" / "-" / ".")

tlsrpt-ext-value  = 1*(%x21-3A / %x3C / %x3E-7E)
                    ; chars excluding "=", ";", SP, and control
                    ; chars
```

If multiple TXT records for "_smtp._tls" are returned by the resolver, records that do not begin with "v=TLSRPTv1;" are discarded. If the number of resulting records is not one, senders MUST assume the recipient domain does not implement TLSRPT. If the resulting TXT record contains multiple strings (as described in Section 3.3 of [RFC7208]), then the record MUST be treated as if those strings are concatenated without adding spaces.

The record supports the ability to declare more than one rua, and if there exists more than one, the reporter MAY attempt to deliver to each of the supported rua destinations. A receiver MAY opt to only attempt delivery to one of the endpoints; however, the report SHOULD NOT be considered successfully delivered until one of the endpoints accepts delivery of the report.

Parsers MUST accept TXT records that are syntactically valid (i.e., valid key/value pairs separated by semicolons) and implement a superset of this specification, in which case unknown fields SHALL be ignored.

3.1. Example Reporting Policy

3.1.1. Report Using MAILTO

```
_smtp._tls.example.com. IN TXT \
        "v=TLSRPTv1;rua=mailto:reports@example.com"
```

3.1.2. Report Using HTTPS

```
_smtp._tls.example.com. IN TXT \
        "v=TLSRPTv1; \
        rua=https://reporting.example.com/v1/tlsrpt"
```

4. Reporting Schema

The report is composed as a plaintext file encoded in the Internet JSON (I-JSON) format [RFC7493].

Aggregate reports contain the following fields:

- o Report metadata:
  - * The organization responsible for the report
  - * Contact information for one or more responsible parties for the contents of the report
  - * A unique identifier for the report
  - * The reporting date range for the report
- o Policy, consisting of:
  - * One of the following policy types: (1) the MTA-STS Policy applied (as a string), (2) the DANE TLSA record applied (as a string, with each RR entry of the RRset listed and separated by a semicolon), and (3) the literal string "no-policy-found", if neither a DANE nor MTA-STS Policy could be found.
  - * The domain for which the policy is applied
  - * The MX host

- Aggregate counts, comprising result type, Sending MTA IP, receiving MTA hostname, session count, and an optional additional information field containing a URI for recipients to review further information on a failure type.

Note that the failure types are non-exclusive; an aggregate report may contain overlapping "counts" of failure types when a single send attempt encountered multiple errors. Reporters may report multiple applied policies (for example, an MTA-STS Policy and a DANE TLSA record for the same domain and MX). Because of this, even in the case where only a single policy was applied, the "policies" field of the report body MUST be an array and not a singular value.

In the case of multiple failure types, the "failure-details" array would contain multiple entries. Each entry would have its own set of information pertaining to that failure type.

4.1. Report Time Frame

The report SHOULD cover a full day, from 00:00-24:00 UTC. This should allow for easier correlation of failure events. To avoid unintentionally overloading the system processing the reports, the reports should be delivered after some delay, perhaps several hours.

As an example, a sending site might want to introduce a random delay of up to four hours:

```
func generate_sleep_delay() {
  min_delay = 1
  max_delay = 14400
  rand = random(min_delay, max_delay)
  return rand
}

func generate_report(policy_domain) {
  do_rpt_work(policy_domain)
  send_rpt(policy_domain)
}

func generate_tlsrpt() {
  sleep(generate_sleep_delay())
  for policy_domain in list_of_tlsrpt_enabled_domains {
    generate_report(policy_domain)
  }
}
```

4.2. Delivery Summary

4.2.1. Success Count

- "total-successful-session-count": This indicates that the Sending MTA was able to successfully negotiate a policy-compliant TLS connection and serves to provide a "heartbeat" to receiving domains that signifies reporting is functional and tabulating correctly. This field contains an aggregate count of successful connections for the reporting system.

4.2.2. Failure Count

- "total-failure-session-count": This indicates that the Sending MTA was unable to successfully establish a connection with the receiving platform. Section 4.3, "Result Types", will elaborate on the failed negotiation attempts. This field contains an aggregate count of failed connections.

4.3. Result Types

The list of result types will start with the minimal set below and is expected to grow over time based on real-world experience. The initial set is outlined in Sections 4.3.1 to 4.3.4:

4.3.1. Negotiation Failures

- "starttls-not-supported": This indicates that the recipient MX did not support STARTTLS.

- "certificate-host-mismatch": This indicates that the certificate presented did not adhere to the constraints specified in the MTA-STS or DANE policy, e.g., if the MX hostname does not match any identities listed in the subject alternative name (SAN) [RFC5280].

- "certificate-expired": This indicates that the certificate has expired.

- "certificate-not-trusted": This is a label that covers multiple certificate-related failures that include, but are not limited to, errors such as untrusted/unknown certification authorities (CAs), certificate name constraints, certificate chain errors, etc. When using this declaration, the reporting MTA SHOULD utilize the "failure-reason-code" to provide more information to the receiving entity.

- "validation-failure": This indicates a general failure for a reason not matching a category above. When using this declaration, the reporting MTA SHOULD utilize the "failure-reason-code" to provide more information to the receiving entity.

4.3.2. Policy Failures

4.3.2.1. DANE-Specific Policy Failures

- "tlsa-invalid": This indicates a validation error in the TLSA record associated with a DANE policy. None of the records in the RRset were found to be valid.

- "dnssec-invalid": This indicates that no valid records were returned from the recursive resolver.

- "dane-required": This indicates that the sending system is configured to require DANE TLSA records for all the MX hosts of the destination domain, but no DNSSEC-validated TLSA records were present for the MX host that is the subject of the report. Mandatory DANE for SMTP is described in Section 6 of [RFC7672]. Such policies may be created by mutual agreement between two organizations that frequently exchange sensitive content via email.

4.3.2.2. MTA-STS-specific Policy Failures

- "sts-policy-fetch-error": This indicates a failure to retrieve an MTA-STS policy, for example, because the policy host is unreachable.

- "sts-policy-invalid": This indicates a validation error for the overall MTA-STS Policy.

- "sts-webpki-invalid": This indicates that the MTA-STS Policy could not be authenticated using PKIX validation.

4.3.3. General Failures

When a negotiation failure cannot be categorized into one of the "Negotiation Failures" stated above, the reporter SHOULD use the "validation-failure" category. As TLS grows and becomes more complex, new mechanisms may not be easily categorized. This allows for a generic feedback category. When this category is used, the reporter SHOULD also use "failure-reason-code" to give some feedback to the receiving entity. This is intended to be a short text field, and the contents of the field should be an error code or error text, such as "X509_V_ERR_UNHANDLED_CRITICAL_CRL_EXTENSION".

4.3.4. Transient Failures

Transient errors due to too-busy networks, TCP timeouts, etc., are not required to be reported.

4.4. JSON Report Schema

The JSON schema is derived from the HTTP Public Key Pinning (HPKP) JSON schema; see Section 3 of [RFC7469].

```
{
  "organization-name": organization-name,
  "date-range": {
    "start-datetime": date-time,
    "end-datetime": date-time
  },
  "contact-info": email-address,
  "report-id": report-id,
  "policies": [{
    "policy": {
      "policy-type": policy-type,
      "policy-string": policy-string,
      "policy-domain": domain,
      "mx-host": mx-host-pattern
    },
    "summary": {
      "total-successful-session-count": total-successful-session-count,
      "total-failure-session-count": total-failure-session-count
    },
    "failure-details": [
      {
        "result-type": result-type,
        "sending-mta-ip": ip-address,
        "receiving-mx-hostname": receiving-mx-hostname,
        "receiving-mx-helo": receiving-mx-helo,
        "receiving-ip": receiving-ip,
        "failed-session-count": failed-session-count,
        "additional-information": additional-info-uri,
        "failure-reason-code": failure-reason-code
        }
      ]
    }
  ]
}
```

JSON Report Format

- "organization-name": The name of the organization responsible for the report. It is provided as a string.

- "date-time": The date-time indicates the start and end times for the report range. It is provided as a string formatted according to "Internet Date/Time Format", Section 5.6 of [RFC3339]. The report should be for a full UTC day, 00:00-24:00.

- "email-address": The contact information for the party responsible for the report. It is provided as a string formatted according to "Addr-Spec Specification", Section 3.4.1 of [RFC5322].

- "report-id": A unique identifier for the report. Report authors may use whatever scheme they prefer to generate a unique identifier. It is provided as a string.

- "policy-type": The type of policy that was applied by the sending domain. Presently, the only three valid choices are "tlsa", "sts", and the literal string "no-policy-found". It is provided as a string.

- "policy-string": An encoding of the applied policy as a JSON array of strings, whether it's a TLSA record ([RFC6698], Section 2.3) or an MTA-STS Policy. Examples follow in the next section.

- "domain": The Policy Domain against which the MTA-STS or DANE policy is defined. In the case of Internationalized Domain Names [RFC5891], the domain MUST consist of the Punycode-encoded A-labels [RFC3492] and not the U-labels.

- "mx-host-pattern": In the case where "policy-type" is "sts", it's the pattern of MX hostnames from the applied policy. It is provided as a JSON array of strings and is interpreted in the same manner as the rules in "MX Host Validation"; see Section 4.1 of [RFC8461]. In the case of Internationalized Domain Names [RFC5891], the domain MUST consist of the Punycode-encoded A-labels [RFC3492] and not the U-labels.

- "result-type": A value from Section 4.3, "Result Types", above.

- "ip-address": The IP address of the Sending MTA that attempted the STARTTLS connection. It is provided as a string representation of an IPv4 (see below) or IPv6 [RFC5952] address in dot-decimal or colon-hexadecimal notation.

- "receiving-mx-hostname": The hostname of the receiving MTA MX record with which the Sending MTA attempted to negotiate a STARTTLS connection.

- "receiving-mx-helo" (optional): The HELLO (HELO) or Extended HELLO (EHLO) string from the banner announced during the reported session.

- "receiving-ip": The destination IP address that was used when creating the outbound session. It is provided as a string representation of an IPv4 (see below) or IPv6 [RFC5952] address in dot-decimal or colon-hexadecimal notation.

- "total-successful-session-count": The aggregate count (an integer, encoded as a JSON number) of successfully negotiated TLS-enabled connections to the receiving site.

- "total-failure-session-count": The aggregate count (an integer, encoded as a JSON number) of failures to negotiate a TLS-enabled connection to the receiving site.

- "failed-session-count": The number of (attempted) sessions that match the relevant "result-type" for this section (an integer, encoded as a JSON number).

- "additional-info-uri" (optional): A URI [RFC3986] that points to additional information around the relevant "result-type". For example, this URI might host the complete certificate chain presented during an attempted STARTTLS session.

- "failure-reason-code": A text field to include a TLS-related error code or error message.

For report purposes, an IPv4 address is defined via the following ABNF:

```
IPv4address = dec-octet "." dec-octet "." dec-octet "." dec-octet
dec-octet     = DIGIT                    ; 0-9
              / %x31-39 DIGIT            ; 10-99
              / "1" 2DIGIT               ; 100-199
              / "2" %x30-34 DIGIT        ; 200-249
              / "25" %x30-35             ; 250-255
```

And an IPv6 address is defined via the following ABNF:

```
IPv6address = <as defined in [RFC5954]>
```

4.5. Policy Samples

Part of the report body includes the policy that is applied when attempting relay to the destination.

For DANE TLSA policies, this is a JSON array of strings each representing the RDATA of a single TLSA resource record as a space-separated list of its four TLSA fields; the fields are in presentation format (defined in [RFC6698], Section 2.2) with no internal spaces or grouping parentheses:

```
[
"3 0 1 1F850A337E6DB9C609C522D136A475638CC43E1ED424F8EEC8513
      D747D1D085D",
"3 0 1 12350A337E6DB9C6123522D136A475638CC43E1ED424F8EEC8513
      D747D1D1234"
]
```

For MTA-STS policies, this is an array of JSON strings that represents the policy that is declared by the receiving site, including any errors that may be present. Note that where there are multiple "mx" values, they must be listed as separate "mx" elements in the policy array rather than as a single nested "mx" sub-array.

```
[
"version: STSv1",
"mode: testing",
"mx: mx1.example.com",
"mx: mx2.example.com",
"mx: mx.backup-example.com",
"max_age: 604800"
]
```

5. Report Delivery

Reports can be delivered either via SMTP (as an email message) or via HTTP POST.

5.1. Report Filename

The filename is RECOMMENDED to be constructed using the following ABNF:

```
filename        = sender "!" policy-domain "!" begin-timestamp
                  "!" end-timestamp [ "!" unique-id ] "." extension

unique-id       = 1*(ALPHA / DIGIT)

sender          = domain ; from [RFC5321] -- this is used
                  ; as the domain for the `contact-info`
                  ; address in the report body.
                  ; In the case of Internationalized Domain
                  ; Names [RFC5891], the domain MUST consist of
                  ; the Punycode-encoded A-labels [RFC3492] and
                  ; not the U-labels.

policy-domain   = domain
                  ; In the case of Internationalized Domain
                  ; Names [RFC5891], the domain MUST consist of
                  ; the Punycode-encoded A-labels [RFC3492] and
                  ; not the U-labels.

begin-timestamp = 1*DIGIT
                  ; seconds since 00:00:00 UTC January 1, 1970
                  ; indicating start of the time range contained
                  ; in the report

end-timestamp   = 1*DIGIT
                  ; seconds since 00:00:00 UTC January 1, 1970
                  ; indicating end of the time range contained
                  ; in the report

extension       = "json" / "json.gz"
```

The extension MUST be "json" for a plain JSON file or "json.gz" for a JSON file compressed using gzip.

"unique-id" allows an optional unique ID generated by the Sending MTA to distinguish among multiple reports generated simultaneously by different sources for the same Policy Domain. For example, this is a possible filename for a compressed report to the Policy Domain "example.net" from the Sending MTA "mail.sndr.example.com":

"mail.sndr.example.com!example.net!1470013207!1470186007!001.json.gz"

5.2. Compression

The report SHOULD be subjected to gzip [RFC1952] compression for both email and HTTPS transport. Declining to apply compression can cause the report to be too large for a receiver to process (a commonly observed receiver limit is ten megabytes); compressing the file increases the chances of acceptance of the report at some computational cost.

5.3. Email Transport

The report MAY be delivered by email. To make the reports machine-parsable for the receivers, we define a top-level media type "multipart/report" with a new parameter "report-type="tlsrpt"". Inside it, there are two parts: The first part is human readable, typically "text/plain", and the second part is machine readable with a new media type defined called "application/tlsrpt+json". If compressed, the report should use the media type "application/tlsrpt+gzip".

In addition, the following two new top-level message header fields are defined:

"TLS-Report-Domain: Receiver-Domain"

"TLS-Report-Submitter: Sender-Domain"

The "TLS-Report-Submitter" value MUST match the value found in the domain [RFC5321] of the "contact-info" from the report body. These message header fields MUST be included and should allow for easy searching for all reports submitted by a reporting domain or a particular submitter, for example, in IMAP [RFC3501]:

"s SEARCH HEADER "TLS-Report-Domain" "example.com""

It is presumed that the aggregate reporting address will be equipped to process new message header fields and extract MIME parts with the prescribed media type and filename, and ignore the rest. These additional headers SHOULD be included in the DKIM [RFC6376] signature for the message.

The RFC5322.Subject field for report submissions SHOULD conform to the following ABNF:

```
    tlsrpt-subject = %s"Report" FWS               ; "Report"
                     %s"Domain:" FWS              ; "Domain:"
                     domain-name FWS              ; per [RFC6376]
                     %s"Submitter:" FWS           ; "Submitter:"
                     domain-name FWS              ; per [RFC6376]
                     %s"Report-ID:" FWS           ; "Report-ID:
                     "<" id-left "@" id-right ">" ; per [RFC5322]
                     [CFWS]                       ; per [RFC5322]
                                                  ; (as with FWS)
```

The first domain-name indicates the DNS domain name about which the report was generated. The second domain-name indicates the DNS domain name representing the Sending MTA generating the report. The purpose of the "Report-ID:" portion of the field is to enable the Policy Domain to identify and ignore duplicate reports that might be sent by a Sending MTA.

For instance, this is a possible Subject field for a report to the Policy Domain "example.net" from the Sending MTA "mail.sender.example.com". It is line-wrapped as allowed by [RFC5322]:

```
           Subject: Report Domain: example.net
               Submitter: mail.sender.example.com
               Report-ID: <735ff.e317+bf22029@mailexample.net>
```

5.3.1. Example Report

```
      From: tlsrpt@mail.sender.example.com
          Date: Fri, May 09 2017 16:54:30 -0800
          To: mts-sts-tlsrpt@example.net
          Subject: Report Domain: example.net
              Submitter: mail.sender.example.com
              Report-ID: <735ff.e317+bf22029@example.net>
          TLS-Report-Domain: example.net
          TLS-Report-Submitter: mail.sender.example.com
          MIME-Version: 1.0
          Content-Type: multipart/report; report-type="tlsrpt";
              boundary="----=_NextPart_000_024E_01CC9B0A.AFE54C00"
          Content-Language: en-us

          This is a multipart message in MIME format.

          ------=_NextPart_000_024E_01CC9B0A.AFE54C00
          Content-Type: text/plain; charset="us-ascii"
          Content-Transfer-Encoding: 7bit

          This is an aggregate TLS report from mail.sender.example.com

          ------=_NextPart_000_024E_01CC9B0A.AFE54C00
          Content-Type: application/tlsrpt+gzip
          Content-Transfer-Encoding: base64
          Content-Disposition: attachment;
              filename="mail.sender.example!example.com!
                        1013662812!1013749130.json.gz"

          <gzipped content of report>

     ------=_NextPart_000_024E_01CC9B0A.AFE54C00--
     ...
```

Note that, when sending failure reports via SMTP, Sending MTAs MUST NOT honor MTA-STS or DANE TLSA failures.

5.4. HTTPS Transport

The report MAY be delivered by POST to HTTPS. If compressed, the report SHOULD use the media type "application/tlsrpt+gzip"; otherwise it SHOULD use the media type "application/tlsrpt+json" (see Section 6, "IANA Considerations").

The receiving system MUST return a "successful" response from its HTTPS server, typically a 200 or 201 HTTP code [RFC7231]. Other codes could indicate a delivery failure and may be retried as per local sender policy. The receiving system is not expected to process reports at receipt time and MAY store them for processing at a later time.

5.5. Delivery Retry

In the event of a delivery failure, regardless of the delivery method, a sender SHOULD attempt redelivery for up to 24 hours after the initial attempt. As previously stated, the reports are optional, so while it is ideal to attempt redelivery, it is not required. If multiple retries are attempted, ideally they SHOULD be done with exponential backoff.

5.6. Metadata Variances

As stated above, there are a variable number of ways to declare information about the data therein. If any of the items declared via subject or filename disagree with the report, the report MUST be considered the authoritative source.

6. IANA Considerations

The following are the IANA considerations discussed in this document.

6.1. Message Headers

Below is the Internet Assigned Numbers Authority (IANA) Permanent Message Header Field registration information per [RFC3864].

```
Header field name:           TLS-Report-Domain
Applicable protocol:         mail
Status:                      standard
Author/Change controller:    IETF
Specification document(s):   RFC 8460


Header field name:           TLS-Report-Submitter
Applicable protocol:         mail
Status:                      standard
Author/Change controller:    IETF
Specification document(s):   RFC 8460
```

6.2. Report Type

This document creates a new registry for the "report-type" parameter to the Content-Type header field for the "multipart/report" top-level media type defined in [RFC6522].

The registry name is "Report Type Registry", and the procedure for updating the registry will be "Specification Required" [RFC8126].

An entry in this registry should contain:

- the report-type being registered
- one or more registered media types that can be used with this report-type
- the document containing the registration action
- an optional comment

The initial entries are:

Report-Type: tlsrpt
Media Type: application/tlsrpt+gzip, application/tlsrpt+json
Registered By: [RFC8460]
Comment: Media types suitable for use with this report-type are defined in Sections 6.4 and 6.5 of [RFC8460]

Report-Type: disposition-notification
Media Type: message/disposition-notification
Registered By: [RFC8098], Section 10

Report-Type: disposition-notification
Media Type: message/global-disposition-notification
Registered By: [RFC6533], Section 6

Report-Type: delivery-status
Media Type: message/delivery-status
Registered By: [RFC3464], Section 6.2

Report-Type: delivery-status
Media Type: message/global-delivery-status
Registered By: [RFC6533], Section 6

6.3. +gzip Media Type Suffix

This document registers a new media type suffix "+gzip". The gzip format is a public domain, cross-platform, interoperable file storage and transfer format, specified in [RFC1952]; it supports compression and is used as the underlying representation by a variety of file formats. The media type "application/gzip" has been registered for such files. The suffix "+gzip" MAY be used with any media type whose representation follows that established for "application/gzip". The registration form for the structured syntax suffix for use with media types is as follows:

Type name: gzip file storage and transfer format.

+suffix: +gzip

References: [RFC1952] [RFC6713]

Encoding considerations: gzip is a binary encoding.

Fragment identifier considerations: The syntax and semantics of fragment identifiers specified for +gzip SHOULD be as specified for "application/gzip". (At publication of this document, there is no fragment identification syntax defined for "application/gzip".) The syntax and semantics for fragment identifiers for a specific "xxx/yyy+gzip" SHOULD be processed as follows:

For cases defined in +gzip, where the fragment identifier resolves per the +gzip rules, process as specified in +gzip.

For cases defined in +gzip, where the fragment identifier does not resolve per the +gzip rules, process as specified in "xxx/yyy+gzip".

For cases not defined in +gzip, process as specified in "xxx/yyy+gzip".

Interoperability considerations: N/A

Security considerations: gzip format doesn't provide confidentiality protection. Integrity protection is provided by an Adler-32 checksum, which is not cryptographically strong. See also the security considerations of [RFC6713]. Each individual media type registered with a +gzip suffix can have additional security considerations. Additionally, gzip objects can contain multiple files and associated paths. File paths must be validated when the files are extracted; a malicious file path could otherwise cause the extractor to overwrite application or system files.

Contact: art@ietf.org

Author/Change controller: Internet Engineering Task Force (iesg@ietf.org).

6.4. application/tlsrpt+json Media Type

This document registers multiple media types, beginning with Table 1 below.

Type	Subtype	File Ext	Specification
application	tlsrpt+json	.json	Section 5.3

Table 1: SMTP TLS Reporting Media Type

Type name: application

Subtype name: tlsrpt+json

Required parameters: N/A

Optional parameters: N/A

Encoding considerations: Encoding considerations are identical to those specified for the "application/json" media type. See [RFC7493].

Security considerations: Security considerations relating to SMTP TLS Reporting are discussed in Section 7.

Interoperability considerations: This document specifies the format of conforming messages and the interpretation thereof.

Published specification: Section 5.3 of RFC 8460.

Applications that use this media type: Mail User Agents (MUAs) and Mail Transfer Agents.

Additional information:

Deprecated alias names for this type: N/A

Magic number(s): N/A

File extension(s): ".json"

Macintosh file type code(s): N/A

Person & email address to contact for further information: See the Authors' Addresses section.

Intended usage: COMMON

Restrictions on usage: N/A

Author: See the Authors' Addresses section.

Change controller: Internet Engineering Task Force (iesg@ietf.org).

6.5. application/tlsrpt+gzip Media Type

Type	Subtype	File Ext	Specification
application	tlsrpt+gzip	.gz	Section 5.3

Table 2: SMTP TLS Reporting Media Type

Type name: application

Subtype name: tlsrpt+gzip

Required parameters: N/A

Optional parameters: N/A

Encoding considerations: Binary

Security considerations: Security considerations relating to SMTP TLS Reporting are discussed in Section 7. Security considerations related to gzip compression are discussed in RFC 6713.

Interoperability considerations: This document specifies the format of conforming messages and the interpretation thereof.

Published specification: Section 5.3 of RFC 8460.

Applications that use this media type: Mail User Agents (MUAs) and Mail Transfer Agents.

Additional information:

Deprecated alias names for this type: N/A

Magic number(s): The first two bytes are 0x1f, 0x8b.

File extension(s): ".gz"

Macintosh file type code(s): N/A

Person & email address to contact for further information: See the Authors' Addresses section.

Intended usage: COMMON

Restrictions on usage: N/A

Author: See the Authors' Addresses section.

Change controller: Internet Engineering Task Force (iesg@ietf.org).

6.6. STARTTLS Validation Result Types

This document creates a new registry, "STARTTLS Validation Result Types". The initial entries in the registry are:

Result Type	Description
starttls-not-supported	Section 4.3
certificate-host-mismatch	Section 4.3
certificate-expired	Section 4.3
tlsa-invalid	Section 4.3
dnssec-invalid	Section 4.3
dane-required	Section 4.3
certificate-not-trusted	Section 4.3
sts-policy-invalid	Section 4.3
sts-webpki-invalid	Section 4.3
validation-failure	Section 4.3
sts-policy-fetch-error	Section 4.3

The above entries are described in Section 4.3, "Result Types". New result types can be added to this registry using the "Expert Review" IANA registration policy.

7. Security Considerations

SMTP TLS Reporting provides visibility into misconfigurations or attempts to intercept or tamper with mail between hosts who support STARTTLS. There are several security risks presented by the existence of this reporting channel:

- Flooding of the Aggregate Report URI (rua) endpoint: An attacker could flood the endpoint with excessive reporting traffic and prevent the receiving domain from accepting additional reports. This type of Denial-of-Service attack would limit visibility into STARTTLS failures, leaving the receiving domain blind to an ongoing attack.

- Untrusted content: An attacker could inject malicious code into the report, exploiting any vulnerabilities in the report-handling systems of the receiving domain. Implementers are advised to take precautions against evaluating the contents of the report.

- Report snooping: An attacker could create a bogus TLSRPT record to receive statistics about a domain the attacker does not own. Since an attacker that is able to poison DNS is already able to receive counts of SMTP connections (and, absent DANE or MTA-STS policies, actual SMTP message payloads), this does not present a significant new vulnerability.

- Ignoring HTTPS validation when submitting reports: When reporting benign misconfigurations, it is likely that a misconfigured SMTP server may also mean a misconfigured HTTPS server; as a result, reporters who require HTTPS validity on the reporting endpoint may fail to alert administrators about such misconfigurations. Conversely, in the event of an actual attack, an attacker who wishes to create a gap in reporting and could intercept HTTPS reports could, just as easily, simply thwart the resolution of the TLSRPT TXT record or establishment of the TCP session to the HTTPS endpoint. Furthermore, such a man-in-the-middle attacker could discover most or all of the metadata exposed in a report merely through passive observation. As a result, we consider the risks of failure to deliver reports on misconfigurations to outweigh those of attackers intercepting reports.

- Reports as DDoS: TLSRPT allows specifying destinations for the reports that are outside the authority of the Policy Domain, which allows domains to delegate processing of reports to a partner organization. However, an attacker who controls the Policy Domain DNS could also use this mechanism to direct the reports to an unwitting victim, flooding that victim with excessive reports. DMARC [RFC7489] defines a solution for verifying delegation to avoid such attacks; the need for this is greater with DMARC, however, because DMARC allows an attacker to trigger reports to a target from an innocent third party by sending mail to that third party (which triggers a report from the third party to the target). In the case of TLSRPT, the attacker would have to induce the third party to send mail to the attacker in order to trigger reports from the third party to the victim; this reduces the risk of such an attack and the need for a verification mechanism.

Finally, because TLSRPT is intended to help administrators discover man-in-the-middle attacks against transport-layer encryption, including attacks designed to thwart negotiation of encrypted connections (by downgrading opportunistic encryption or, in the case of MTA-STS, preventing discovery of a new MTA-STS Policy), we must also consider the risk that an adversary who can induce such a downgrade attack can also prevent discovery of the TLSRPT TXT record (and thus prevent discovery of the successful downgrade attack). Administrators are thus encouraged to deploy TLSRPT TXT records with a large TTL (reducing the window for successful application of transient attacks against DNS resolution of the record) or to deploy DNSSEC on the deploying zone.

8. Privacy Considerations

MTAs are generally considered public knowledge; however, the internals of how those MTAs are configured and the users of those MTAs may not be as public. It should be noted that providing a receiving site with information about TLS failures may reveal information about the sender's configuration or even information about the senders themselves. For example, sending a report may disclose what TLS implementation the sender uses, as the inability to negotiate a session may be a known incompatibility between two implementations. This may, indirectly, leak information on the reporter's operating system or even region, if, for example, a rare TLS implementation is popular among certain users or in certain locations.

9. References

9.1. Normative References

[RFC1952] Deutsch, P., "GZIP file format specification version 4.3", RFC 1952, DOI 10.17487/RFC1952, May 1996, <https://www.rfc-editor.org/info/rfc1952>.

[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>.

[RFC3339] Klyne, G. and C. Newman, "Date and Time on the Internet: Timestamps", RFC 3339, DOI 10.17487/RFC3339, July 2002, <https://www.rfc-editor.org/info/rfc3339>.

[RFC3492] Costello, A., "Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA)", RFC 3492, DOI 10.17487/RFC3492, March 2003, <https://www.rfc-editor.org/info/rfc3492>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <https://www.rfc-editor.org/info/rfc3986>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <https://www.rfc-editor.org/info/rfc5234>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008, <https://www.rfc-editor.org/info/rfc5321>.

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, DOI 10.17487/RFC5322, October 2008, <https://www.rfc-editor.org/info/rfc5322>.

[RFC5891] Klensin, J., "Internationalized Domain Names in Applications (IDNA): Protocol", RFC 5891, DOI 10.17487/RFC5891, August 2010, <https://www.rfc-editor.org/info/rfc5891>.

[RFC5952] Kawamura, S. and M. Kawashima, "A Recommendation for IPv6 Address Text Representation", RFC 5952, DOI 10.17487/RFC5952, August 2010, <https://www.rfc-editor.org/info/rfc5952>.

[RFC6068] Duerst, M., Masinter, L., and J. Zawinski, "The 'mailto' URI Scheme", RFC 6068, DOI 10.17487/RFC6068, October 2010, <https://www.rfc-editor.org/info/rfc6068>.

[RFC6376] Crocker, D., Ed., Hansen, T., Ed., and M. Kucherawy, Ed., "DomainKeys Identified Mail (DKIM) Signatures", STD 76, RFC 6376, DOI 10.17487/RFC6376, September 2011, <https://www.rfc-editor.org/info/rfc6376>.

[RFC6522] Kucherawy, M., Ed., "The Multipart/Report Media Type for the Reporting of Mail System Administrative Messages", STD 73, RFC 6522, DOI 10.17487/RFC6522, January 2012, <https://www.rfc-editor.org/info/rfc6522>.

[RFC6698] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, DOI 10.17487/RFC6698, August 2012, <https://www.rfc-editor.org/info/rfc6698>.

[RFC6713] Levine, J., "The 'application/zlib' and 'application/gzip' Media Types", RFC 6713, DOI 10.17487/RFC6713, August 2012, <https://www.rfc-editor.org/info/rfc6713>.

[RFC7208] Kitterman, S., "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1", RFC 7208, DOI 10.17487/RFC7208, April 2014, <https://www.rfc-editor.org/info/rfc7208>.

[RFC7231] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content", RFC 7231, DOI 10.17487/RFC7231, June 2014, <https://www.rfc-editor.org/info/rfc7231>.

[RFC7405] Kyzivat, P., "Case-Sensitive String Support in ABNF", RFC 7405, DOI 10.17487/RFC7405, December 2014, <https://www.rfc-editor.org/info/rfc7405>.

[RFC7493] Bray, T., Ed., "The I-JSON Message Format", RFC 7493, DOI 10.17487/RFC7493, March 2015, <https://www.rfc-editor.org/info/rfc7493>.

[RFC7671] Dukhovni, V. and W. Hardaker, "The DNS-Based Authentication of Named Entities (DANE) Protocol: Updates and Operational Guidance", RFC 7671, DOI 10.17487/RFC7671, October 2015, <https://www.rfc-editor.org/info/rfc7671>.

[RFC7672] Dukhovni, V. and W. Hardaker, "SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS)", RFC 7672, DOI 10.17487/RFC7672, October 2015, <https://www.rfc-editor.org/info/rfc7672>.

[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>.

[RFC8461] Margolis, D., Risher, M., Ramakrishnan, B., Brotman, A., and J. Jones, "SMTP MTA Strict Transport Security (MTA-STS)", RFC 8461, DOI 10.17487/RFC8461, September 2018, <https://www.rfc-editor.org/info/rfc8461>.

9.2. Informative References

[RFC3207] Hoffman, P., "SMTP Service Extension for Secure SMTP over Transport Layer Security", RFC 3207, DOI 10.17487/RFC3207, February 2002, <https://www.rfc-editor.org/info/rfc3207>.

[RFC3464] Moore, K. and G. Vaudreuil, "An Extensible Message Format for Delivery Status Notifications", RFC 3464, DOI 10.17487/RFC3464, January 2003, <https://www.rfc-editor.org/info/rfc3464>.

[RFC3501] Crispin, M., "INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1", RFC 3501, DOI 10.17487/RFC3501, March 2003, <https://www.rfc-editor.org/info/rfc3501>.

[RFC3864] Klyne, G., Nottingham, M., and J. Mogul, "Registration Procedures for Message Header Fields", BCP 90, RFC 3864, DOI 10.17487/RFC3864, September 2004, <https://www.rfc-editor.org/info/rfc3864>.

[RFC6533] Hansen, T., Ed., Newman, C., and A. Melnikov, "Internationalized Delivery Status and Disposition Notifications", RFC 6533, DOI 10.17487/RFC6533, February 2012, <https://www.rfc-editor.org/info/rfc6533>.

[RFC7435] Dukhovni, V., "Opportunistic Security: Some Protection Most of the Time", RFC 7435, DOI 10.17487/RFC7435, December 2014, <https://www.rfc-editor.org/info/rfc7435>.

[RFC7469] Evans, C., Palmer, C., and R. Sleevi, "Public Key Pinning Extension for HTTP", RFC 7469, DOI 10.17487/RFC7469, April 2015, <https://www.rfc-editor.org/info/rfc7469>.

[RFC7489] Kucherawy, M., Ed. and E. Zwicky, Ed., "Domain-based Message Authentication, Reporting, and Conformance (DMARC)", RFC 7489, DOI 10.17487/RFC7489, March 2015, <https://www.rfc-editor.org/info/rfc7489>.

[RFC8098] Hansen, T., Ed. and A. Melnikov, Ed., "Message Disposition Notification", STD 85, RFC 8098, DOI 10.17487/RFC8098, February 2017, <https://www.rfc-editor.org/info/rfc8098>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

Appendix A. Example Reporting Policy

A.1. Report Using MAILTO

```
_smtp._tls.mail.example.com. IN TXT \
        "v=TLSRPTv1;rua=mailto:reports@example.com"
```

A.2. Report Using HTTPS

```
_smtp._tls.mail.example.com. IN TXT \
        "v=TLSRPTv1; \
        rua=https://reporting.example.com/v1/tlsrpt"
```

Appendix B. Example JSON Report

Below is an example JSON report for messages from Company-X to Company-Y, where 100 sessions were attempted to Company-Y servers with an expired certificate, and 200 sessions were attempted to Company-Y servers that did not successfully respond to the "STARTTLS" command. Additionally, 3 sessions failed due to "X509_V_ERR_PROXY_PATH_LENGTH_EXCEEDED".


```
{
  "organization-name": "Company-X",
  "date-range": {
    "start-datetime": "2016-04-01T00:00:00Z",
    "end-datetime": "2016-04-01T23:59:59Z"
  },
  "contact-info": "sts-reporting@company-x.example",
  "report-id": "5065427c-23d3-47ca-b6e0-946ea0e8c4be",
  "policies": [{
    "policy": {
      "policy-type": "sts",
      "policy-string": ["version: STSv1","mode: testing",
            "mx: *.mail.company-y.example","max_age: 86400"],
      "policy-domain": "company-y.example",
      "mx-host": "*.mail.company-y.example"
    },
    "summary": {
      "total-successful-session-count": 5326,
      "total-failure-session-count": 303
    },
    "failure-details": [{
      "result-type": "certificate-expired",
      "sending-mta-ip": "2001:db8:abcd:0012::1",
      "receiving-mx-hostname": "mx1.mail.company-y.example",
      "failed-session-count": 100
    }, {
```

```
        "result-type": "starttls-not-supported",
        "sending-mta-ip": "2001:db8:abcd:0013::1",
        "receiving-mx-hostname": "mx2.mail.company-y.example",
        "receiving-ip": "203.0.113.56",
        "failed-session-count": 200,
        "additional-information": "https://reports.company-x.example/
          report_info ? id = 5065427 c - 23 d3# StarttlsNotSupported "
      }, {
        "result-type": "validation-failure",
        "sending-mta-ip": "198.51.100.62",
        "receiving-ip": "203.0.113.58",
        "receiving-mx-hostname": "mx-backup.mail.company-y.example",
        "failed-session-count": 3,
        "failure-reason-code": "X509_V_ERR_PROXY_PATH_LENGTH_EXCEEDED"
      }]
    }]
  }
```

Contributors

Laetitia Baudoin
Google, Inc.
lbaudoin@google.com

Authors' Addresses

Daniel Margolis
Google, Inc.

Email: dmargolis@google.com

Alexander Brotman
Comcast, Inc.

Email: alex_brotman@comcast.com

Binu Ramakrishnan
Oath, Inc.

Email: prbinu@yahoo.com

Janet Jones
Microsoft, Inc.

Email: janet.jones@microsoft.com

Mark Risher
Google, Inc.

Email: risher@google.com