TLS Reporting (TLSRPT)

Carsten Strotmann - Patrick Koetter, sys4 AG

CREATED: 2023-10-20 FRI 12:29

TLSRPT

The problem

- Detecting issues with SMTP transport security can be difficult
    - The issues are only visible on the sending side
    - The issues might be present on the receiving side

The solution

- TLS Reporting (TLSRPT, RFC 8460 Standards Track) defines a protocol for communicating TLS issues from a sending MTA towards the operator of the receiving MTA
- TLSRPT helps finding issues with both DANE (RFC 6698 Standards Track) and MTA-STS (RFC 8461 Standards Track)
    - failures in routing
    - failures in DNS resolution
    - failures in TLS/STARTTLS negotiation
- TLSRPT works very similar to DMARC (RFC 7489 Standards Track) reporting

How TLSRPT works

TLSRPT in pictures (1)

TLSRPT in pictures (2)

TLSRPT in pictures (3)

TLSRPT DNS Record

- The TLS reporting policy is published with a DNS TXT record at the DNS label **`_smtp._tls`** at the mail domain. For the mail-domain **`example.org`** the domain name for the TXT record would be **`_smtp._tls.example.org`**.

TLSRPT record values

- The TLSRPT record contains key/value-pairs (separated by semicolon):
  - **v**: TLSRPT version number, current value **`TLSRPTv1`**
  - **rua**: Reporting URI, either of type *mailto* (report via SMTP mail) or *https* (HTTP-Post). There can be multiple **rua** values in the TLSRPT TXT record

Example TLSRPT

```
; <<>> DiG 9.16.44-Debian <<>> _smtp._tls.google.com txt
[...]
;; ANSWER SECTION:
_smtp._tls.google.com.  360     IN      TXT     "v=TLSRPTv1;rua=mailto:sts-reports@google.com"
```

TLSRPT report format

TLSRPT report format

- The TLSRPT aggregate reports are send as compressed (*gzip*) JSON documents (`application/tlsrpt+json` mime type)
- Each aggregated report should cover 24 hours (the reporting software needs to collect TLSRPT data for this time to generate the reports)

TLSRPT metadata

- The TLSRPT aggregate report contains metadata
  - Information on the organization sending the report
  - Contact information for the responsible operators for the content of the report
  - A unique identifier for the report
  - The date range contained in the report

TLSRPT policy data

- Applied policy
  - DANE, including the used TLSA records
  - MTA-STS, including the content of the MTA-STS policy document
  - The text **`no-policy-found`** if neither DANE nor MTA-STS have been found

- The MX host where the TLS issue has been found
- The mail domain where the issue has been seen
- Aggregate counts of issues

TLS negotiation failure types reported

REPORTED FAILURE	DESCRIPTION
starttls-not-supported	Receiver does not offer STARTTLS
certificate-host-mismatch	Domain name(s) in the receiving MTA certificate do not match the DNS name of the MTA
certificate-expired	The certificate is expired
certificate-not-trusted	The certificate does not contain a valid trust chain towards a trusted root CA
validation-failure	The certificate could not be validated

DANE negotiation failure types reported

REPORTED FAILURE	DESCRIPTION
tlsa-invalid	The TLSA record found in DNS is invalid
dnssec-invalid	The DNSSEC validation on the TLSA record failed
dane-required	The sending MTA is configured to require mandatory DANE security for this mail destination. Mandatory DANE for SMTP is described in Section 6 of RFC7672

MTA-STS negotiation failure types reported

REPORTED FAILURE	DESCRIPTION
sts-policy-fetch-error	The MTA-STS policy cannot be loaded from the web server (document does not exist or other http error)
sts-policy-invalid	The MTS-STS policy document cannot be parsed, it is invalid
sts-webpki-invalid	The TLS connection to the web-server containing the MTA-STS document cannot be established

Implementing TLSRPT

TLSRPT security

- To prevent resource exhaustion attacks on mail infrastructure, the reporting part for TLSRPT should be decoupled from the sending mail server infrastructure
- Reports should be collected and send as a batch to the receiving side to not overload the receiving infrastructure
- TLSRPT does not require DNSSEC security for the TXT-Record

TLSRPT privacy

- Reporting can leak sensitive information
  - Failure reports from the sender to the receiver can leak internal information on the TLS implementation and the MTA product being used
  - Information about the senders email address or even part of the message might end up in the reporting
  - TLSRPT reporting functions of MTAs should be evaluated for possible privacy issues

TLSRPT implementations

- Open Source:
  - together with Wietse Venema (Postfix), sys4 is currently developing a low-level C library that can be integrated into any MTA (Postfix, Sendmail, Exim, ...) as well as TLSRPT data receiver and reporter services that can aggregate TLSRPT report data, process it into a report and transmit it. (ETA Q1 / 2024)
  - DMARC & SMTP-TLS Reports processor and visualizer: https://github.com/antedebaas/DMARC-SMTPTLS-Reports
  - Simple python script to process TLSRPT reports https://github.com/Comcast/tlsrpt_processor

TLSRPT implementations

- All large mail platforms (gmail, microsoft, yahoo, ...) have implemented TLSRPT

External TLSRPT services

- DMarcian
- PowerDMARC
- Redshift
- and more

End

Questions? / Answers!