

Improving security of email in transit  
with SMTP MTA Strict Transport  
Security (STS)

IETF 98 - March 28, 2017

# Overview

Two separate, compatible specs:

- **TLSRPT:** reporting of TLS negotiation failures
  - Also compatible with DANE
- **MTA-STS:** enforcing TLS+authentication for SMTP

# Threat Model

**Status quo (absent DANE!):**

```
MTA ---MX lookup---> DNS // MX injection (absent DNSSEC)
MTA ---EHLO-----> MTA // Host injection
MTA ---STARTTLS----> MTA // MITM can downgrade
MTA <--server cert-- MTA // No cert validation
```

Opportunistic encryption: Good, but weak against

- active MITM
- DNS injection
- BGP trickery

(like a state- or ISP-level adversary)

# As seen in the wild



Top 10 countries by fraction of incoming Gmail messages that originate from the IPs stripping TLS from SMTP connections.

Country	% of inbound traffic
Tunisia	96.13%
Iraq	25.61%
Papua New Guinea	25.00%
Nepal	24.29%
Kenya	24.13%
Uganda	23.28%
Lesotho	20.25%
Sierra Leone	13.41%
New Caledonia	10.13%
Zambia	9.98%

# STS in 60 Seconds...

1. TXT record

```
$ dig -t txt +short _mta-sts.example.com.
```

```
"v=STSV1; id=20160707T010757;"
```

2. HTTPS endpoint with policy

```
$ curl  
https://mta-sts.example.com/.well-known/mta-sts.json
```

```
{  
  "version": "STSV1",  
  "mode": "report",  
  "mx": ["*.example.com"],  
  "max_age": 123456  
}
```

Semantics:

- HTTPS cert validation
- HSTS-style policy cache
- "Report" or "enforce"

# TLSRPT in 5 seconds...

1. TXT record

```
$ dig -t txt +short _smtp-tlsrpt.example.com.
```

```
"v=TLSRPTv1;rua=mailto:rpt@example.com"
```

2. Reports

```
"Failure-details": [
```

```
{
```

```
  "result-type":
```

```
  "StarttlsNotSupported",
```

```
  "sending-mta-ip": "98.22.33.99",
```

```
  "Session-count": 1000,
```

```
  "receiving-mx-hostname":
```

```
    "mx2.mail.company-y.com",
```

```
  "receiving-mx-helo":
```

```
    "mx2011.mail.company-y.com",
```

```
  ...
```

```
}]
```

# Current Status

- Current drafts have been reviewed by IETF UTA workgroup
  - SMTP MTA Strict Transport Security [draft-ietf-uta-mta-sts-03](#)
  - SMTP TLS Reporting [draft-ietf-uta-smtp-tlsrpt-03](#)
- Incorporating feedback from UTA mailing list
- Pilot implementations underway
- Working towards last call--**pending questions in next slides**

# Open Question #1: Policy Format

- Currently JSON:
  - Pros: Standards-track (RFC 7159), widely implemented in libraries
  - Cons: Not widely implemented in MTAs
  
- Suggested alternative is key=value pairs:
  - Pros: Widely implemented by MTAs
  - Cons: Potentially less extensible, potentially involves handwritten parsers



## Open Question #2: "host" or "identity"

(Mostly resolved in favor of option 2...)

```
mx: [".example.com"]
```

- pattern currently constrains MX *hostnames*:
  - "dig -t mx example.com" → mx1.example.com, mx2.example.com
  - Pros: Easy to implement cert matching ("does it match host?")
  - Cons: Modifies MX list traversal behavior
- Alternative: pattern constrains CN/SAN of server cert
  - Ensure cert has a SAN with a DNS-ID that matches the MX patterns
  - Pros: Easy to implement MX bits (no changes!)
  - Cons: Custom matching "mx" pattern against SAN/CN
    - Wildcard-to-wildcard matching?

# Implementation stages

## Reporting:

- Can be implemented without STS
- Reports can be generated offline (but to report STS or TLSA failures, cert logging/evaluation needed)
- **Very low bar. If you do nothing, receive reports!**

## STS:

- Publishing a policy is easy (just a TXT and HTTPS endpoint...if you have a valid cert)
- **Do this and senders can validate and generate reports!**
- Enforcement requires code in your MTA...

# Known Current Efforts

- Google
  - Policy is live <https://mta-sts.gmail.com/.well-known/mta-sts.json>
  - Send-time validation in progress
- Microsoft
  - Policy publication in progress
- Comcast
  - Policy is live <https://mta-sts.comcast.net/.well-known/mta-sts.json>
  - HTTPS in progress, report processing planned
- Yahoo
  - Policy is live <https://mta-sts.yahoo.com/.well-known/mta-sts.json>
  - Report-only mode in progress
- 1&1
  - Report-only mode in progress
- Fraudmarc
  - Policy is live for ESP pilot; creating 3rd party integration tools

<https://www.fraudmarc.com/sntp-mta-sts-policy-check/>



[DMARC Check](#)

[SPF Record Check](#)

[Got DMARC?](#)

[Contact](#)

Lookup a domain's  
MTA-STS Policy

MailChimp.com

🔍 CHECK

Valid policy located

```
id: 20161021T140000
mode (report or enforce): report
max_age: 30
authorized mx: aspmx1.google.com
authorized mx: alt1.aspmx1.google.com
authorized mx: alt2.aspmx1.google.com
authorized mx: aspmx2.googlemail.com
authorized mx: aspmx3.googlemail.com
```

# Call to Action

- Submit any final feedback to the UTA mailing list