SMTP Security Options

Wes Hardaker
USC/ISI
<hardaker@isi.edu>

Viktor Dukhovni
Two Sigma
<ietf-dane@dukhovni.org>

ICANN65 | Marrakesh, Morocco | June 2019

Overview

1. SMTP (Insecurity) Review
2. E-Mail Security with DANE
3. E-Mail Security with MTA-STS
4. Comparison of DANE and MTA-STS

Email Security

Sending
Mail Server

1. User sends mail
to their outgoing
mail server

**Authenticated SMTP
over authenticated TLS**

Receiving
Mail Server

3. User receives mail
from their incoming
mail server

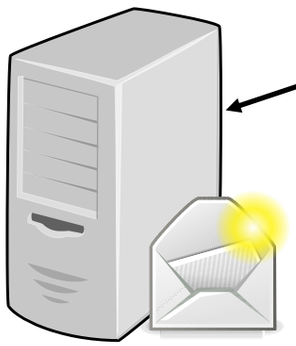
**Authenticated IMAP
over authenticated TLS**

Email Security

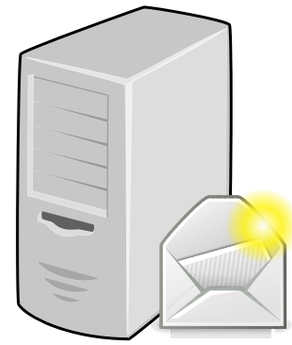
2. MTA-to-MTA SMTP

Then a miracle occurs

Sending Mail Server



Receiving Mail Server



1. User sends mail to their outgoing mail server

Authenticated SMTP over authenticated TLS

3. User receives mail from their incoming mail server

Authenticated IMAP over authenticated TLS

Email Security

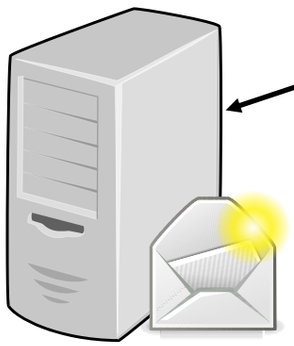
F
6/10

"I think you should be more explicit here in step two."

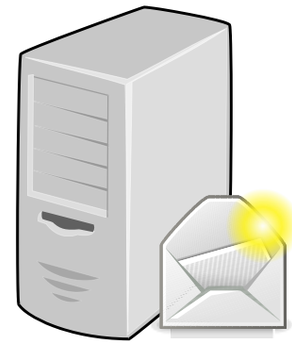
2. MTA-to-MTA SMTP

Then a miracle occurs

Sending Mail Server



Receiving Mail Server



1. User sends mail to their outgoing mail server

Authenticated SMTP over authenticated TLS

3. User receives mail from their incoming mail server

Authenticated IMAP over authenticated TLS

Email Security

Sending Mail Server

How do we establish a secure TLS session to deliver the mail?

Receiving Mail Server

Typical DNS lookups for Mail Transport Agents (MTAs):

1) Lookup *"example.com/MX"* to get a prioritized list of mail servers.

Example records for icann.org:

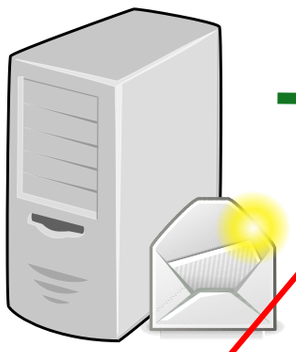
```
icann.org.      600   IN MX 10 pechora2.icann.org.
icann.org.      600   IN MX 10 pechora6.icann.org.
icann.org.      600   IN MX 10 pechora1.icann.org.
icann.org.      600   IN MX 10 pechora8.icann.org.
```

2) Start with the best (lowest) priority, looking up their address

```
pechora2.icann.org.3600 IN AAAA 2620:0:2d0:201::1:72
```

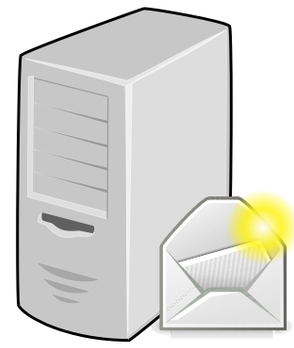
Mail Transport Agents

Sending Mail Server



How do we establish a secure TLS session to deliver the mail?

Receiving Mail Server



Typical DNS lookups for Mail Transport Agents (MTAs):

1) Lookup *"example.com/MX"* to get a prioritized list of mail servers.

Example records for icann.org:

```
icann.org.      600   IN MX 10 pechora2.icann.org.
icann.org.      600   IN MX 10 pechora6.icann.org.
icann.org.      600   IN MX 10 pechora1.icann.org.
icann.org.      600   IN MX 10 pechora8.icann.org.
```

2) Start with the best (lowest) priority, looking up their address

```
pechora2.icann.org.3600 IN AAAA 2620:0:2d0:201::1:72
```

Insecure Without DNSSEC!!

Original SMTP: Insecure

Sending Mail Server

How do we establish a secure TLS session to deliver the mail?

Receiving Mail Server

Why is it insecure???

Sending server: I support TLS
Receiving server: I too support TLS

Man in the middle: Hides receiver capability
Sending server: goes ahead in the clear

We need a way to securely signal “I support TLS”

DANE/SMTP to the Rescue (IETF RFC 7672)

ICANN65 | Marrakesh, Morocco | June 2019

Email Security

Sending Mail Server

How do we establish a secure TLS session to deliver the mail?

Receiving Mail Server

1) Lookup *"ietf.org/MX"*

```
ietf.org.   300  IN MX 0 mail.ietf.org.
```

2) Start with the best (lowest) priority, looking up their address

```
mail.ietf.org.   300  IN AAAA 2001:1900:3001:11::2c
```

3)Look up their TLSA (DANE) record

```
_25._ttcp.mail.ietf.org.262  IN TLSA 3 1 1
0C72AC70B745AC19998811B131D662C9AC69DBDBE7CB23E5B514
B566 64C5D3D6
```

Email Security

Sending Mail Server

How do we establish a secure TLS session to deliver the mail?

Receiving Mail Server

3) Look up their TLSA (DANE) record

```
_25._tcp.mail.ietf.org. 262  IN TLSA 3 1 1
0C72AC70B745AC19998811B131D662C9AC69DBDBE7CB23E5B514
B566  64C5D3D6
```

- AHA! Now I **know** you do TLS
  - DNSSEC proves it exists

- If the TLSA record doesn’t exist:
  - AHA! Now I know all hope is lost
  - **ONLY DNSSEC provides proof of non-existence**

DANE/SMTP Provides

1. Proof of existence
2. Proof of the right TLS end-point
3. Proof when security isn’t available
4. But… it requires DNSSEC

Enter MTA-STS
(IETF RFC 8461)

ICANN65 | Marrakesh, Morocco | June 2019

What if you can’t do DNSSEC?

RFC-8461

SMTP MTA Strict Transport Security (MTA-STS)

“The primary motivation of MTA-STS is to provide a mechanism for domains to ensure transport security even when deploying DNSSEC is undesirable or impractical.”

Goal: don’t require DNSSEC

Email Security

Sending Mail Server

How do we establish a secure TLS session to deliver the mail?

Receiving Mail Server

1) Lookup *"ietf.org/MX"*

```
google.com.    600   IN MX 10 aspmx.l.google.com.
```

2) Start with the lowest priority, looking up their address

```
aspmx.l.google.com. 293   IN AAAA 2607:f8b0:400e:c08::1a
```

3)Lookup their MTA-STS record

```
_mta-sts.google.com.  300   IN TXT
    "v=STSv1; id=20190429T010101;"
```

Email Security

Sending Mail Server

How do we establish a secure TLS session to deliver the mail?

Receiving Mail Server

1) Lookup *“ietf.org/MX”*

2) Start with the lowest priority, looking up their address

3)Lookup their MTA-STS record

```
_mta-sts.google.com.  300  IN TXT
    "v=STSv1; id=20190429T010101;"
```

4)Fetch their policy from https://mta-sts.google.com/.well-known/mta-sts.txt

MTA-STS Record Example: Google

```
version: STSv1
mode: enforce
mx: aspmx.l.google.com
mx: *.aspmx.l.google.com
max_age: 86400
```

MTA-STS Record Example: Google

```
version: STSv1
mode: enforce
mx: aspmx.l.google.com
mx: *.aspmx.l.google.com
max_age: 86400
```

- **mode** selects how “production” you want to be:
  - mode = enforce | testing | none
  - *Testing:* report failures but send mail anyway
  - *None:* used for removal of MTA-STS (more later)

MTA-STS Record Example: Google

```
version: STSv1
mode: enforce
mx: aspmx.l.google.com
mx: *.aspmx.l.google.com
max_age: 86400
```

- **mx** lists all the legitimate hosts to connect to
  - Exact match
  - Or a * to match any label at that point

MTA-STS Record Example: Google

```
version: STSv1
mode: enforce
mx: aspmx.l.google.com
mx: *.aspmx.l.google.com
max_age: 86400
```

- **max_age** specifies lifetime of the policy after being fetched
  - Store it this long since the last time you checked it
  - Different than the DNS TTL!

MTA-STS Fetching Process

1) Check for a valid, cached policy for an MX
   - If none, attempt to fetch TXT/HTTPS
   - Optionally asynchronously
2) For each MX in priority order:
    1) Attempt delivery
    2) If policy is **enforce**, ensure *STARTTLS* and identity
    3) Deliver and stop on success
    4) Treat *invalid* an unreachable
3) If fail on all MX, recheck DNS for a newer policy

Changing or Deleting an MTA-STS Policy

Must follow a proper order:

1) Publish a new HTTPS policy
   - Set to "*mode: none*" to start removal if desired

2) Update the TXT record

3) If deleting:
   - After all policies have expired, remove the TXT record

DANE/SMTP and MTA-STS Comparison

ICANN65 | Marrakesh, Morocco | June 2019

DANE/SMTP and MTA-STS Comparison

Topic	DANE/SMTP	MTA-STS
Definition	RFC 7672	RFC 8461
Protocols	DNS	DNS / HTTPS
Requires DNSSEC	YES	NO
Requires X.509 CAs	Optional	YES
Testing options	Partial deployment (some MXs)	“testing” policy
Record TYPE	TLSA	TXT
Fail soft	NO	YES
Trust Anchors	DNSSEC	All X.509 CAs
Revocation	DNSSEC TTLs	“MAY” check certificate revocation
TLS requirements	unspecified	1.2+
Software support	Open Source (postfix, exim)	Proprietary only

Notable Differences: Downgrade Resistance

- **DANE:**
  - Impossible to remove a DNSSEC signed record
  - Secure on first look-up
- **MTA-STS:**
  - Policy dictates how long records are cached
  - “Leap of faith” style security
    - (only secure after the first look up)
    - Security can expire for infrequent destinations
  - “The mail must go through”
    - Certificate revocation checks are optional
    - If you can’t fetch policy, send anyway

Notable Differences: Scalability

- **Protecting one domain:**
  - **DANE:**
    - Add TLS certificate to MTA
    - Add TLSA record
  - **MTA-STS:**
    - Add TLS certificate to MTA
    - Add HTTPS site
    - Add TXT record
- **Protecting a second domain, with the same MTA**
  - **DANE:**
    - Nothing to do! (the TLSA record already covers it)
  - **MTA-STS:**
    - Add new HTTPS site (with new certificate)
    - Add new TXT record

Which to use?

- Simply put: **DANE/SMTP is more secure**
- The MTA-STS RFC acknowledges this:

> “DANE requires DNSSEC [RFC4033] for authentication; the mechanism described here instead relies on certification authorities (CAs) and does not require DNSSEC, at a cost of risking malicious downgrades.”

> “senders who implement MTA-STS validation MUST NOT allow MTA-STS Policy validation to override a failing DANE validation.”

Questions
?