Using DNSSEC and DANE to prevent email interception

Nordic Domain Days 2018

Vittorio Bertola
Head of Policy & Innovation, Open-Xchange

20 November 2018
State of email transport security
End-to-end email encryption

• Very little end-user adoption of E2E encryption in Email
  • Works in closed environments, not globally

• E2E Email Encryption is hampered by many factors:
  • Open Standards - thousands of service providers, many vendors
  • Existing standards are not geared towards naïve users
  • Key distribution/lookup problem (also, “managed” end-to-end is not end-to-end)
  • Competing standards (S/MIME, OpenPGP)
  • And now, potential security issues (Efail)
Email transport encryption

- STARTTLS Extension allows TLS negotiation for SMTP Sessions
- Most MTAs support STARTTLS
  - Any SMTP Transport Session has the capability to be encrypted

- The growth in transport encryption since 2014 has been significant
  - Incoming (= actually activated) has reached outgoing (= supported)
  - Both percentages now at around 90%
  - Email is less encrypted on Sundays
Gmail: Outgoing email using TLS
Gmail: Incoming email using TLS
Attacks to email transport encryption

• STARTTLS is optional
  • Unencrypted is *always* available as a fallback (unless explicitly disabled)
  • Thus **MITM downgrade attacks** to get transmission in cleartext are trivial
  • People are unable to disable cleartext due to that 10%, which is not going away

• Most MTAs do not authenticate the receiving server
  • Certificate validation is very rare and often does not even work
  • Little incentive to do authentication when the only option is to fallback to cleartext
  • STARTTLS vulnerable to **spoofed MX record attack**
Normal STARTTLS negotiation

1. Sending MTA: EHLO sender.com
2. Receiving MTA: Certificate for rcpt.com
3. STARTTLS
4. 250 STARTTLS
5. ENCRYPTED TRAFFIC
STARTTLS MITM downgrade attack

Sending MTA

EHLO sender.com

250 rcpt.com

CLEARTEXT

Attacker’s MTA

EHLO sender.com

250 STARTTLS

CLEARTEXT

Receiving MTA
DNS cache poisoning attack against MXs

DNS resolver

MX rcpt.com?

MX 5 mx.attacker.com

EHLO sender.com

STARTTLS

250 STARTTLS

Certificate for attacker.com

Attacker’s MTA

Sending MTA

Receiving MTA

Cache poisoning attack

DNS cache poisoning

ENCRYPTED TRAFFIC
Certificate validation is futile

- Majority of mail servers present certificates that cannot be validated correctly

<table>
<thead>
<tr>
<th></th>
<th>Matches Domain</th>
<th>Matches Server</th>
<th>Matches Neither</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted</td>
<td>4,602 (0.6%)</td>
<td>270,723 (34.2%)</td>
<td>143,113 (18.1%)</td>
</tr>
<tr>
<td>Untrusted</td>
<td>4,345 (0.6%)</td>
<td>21,057 (2.7%)</td>
<td>181,242 (22.9%)</td>
</tr>
<tr>
<td>Total</td>
<td>8,947 (1.1%)</td>
<td>291,780 (36.8%)</td>
<td>324,355 (41.0%)</td>
</tr>
</tbody>
</table>

- \textit{Trusted} means that the certificate is signed by a trusted CA
- Results are unsurprising given the lack of validation in MTAs
  - Exim, Sendmail, Qmail and Exchange do not support validating dest domain in cert
  - Postfix docs recommend against it

Source:
"Neither Snow nor Rain not MITM... An Empirical Analysis of Email Delivery Security"
Proceedings of the 2015 Internet Measurement Conference
Security problems with TLS configurations

• Many installations using old TLS versions and insecure ciphersuites
  • Almost half of all incoming encrypted connections to Gmail still use RC4
  • Unknown how many are using even older ciphersuites (old defaults etc.)
  • Configuration of ciphersuites is important but rarely done properly

• Some large installations have middleboxes (e.g. load balancers) that act as MITM
  • May offload STARTTLS to middlebox
  • Managed by different team, may have no control over ciphers, certificates etc.
TLS versions used in transport

- TLS 1.2: 57.9%
- TLS 1.1: 13.7%
- TLS 1.0: 6.8%
- No TLS: 21.6%

Source: Analysis on top 1000 domains by web traffic, TES Tool, May 2017

~10% of those supporting TLS still offer authentication before STARTTLS
Algorithms used for TLS encryption

<table>
<thead>
<tr>
<th>TLS Version</th>
<th>Key Exchange</th>
<th>Symmetric Cipher</th>
<th>HMAC</th>
<th>Inbound Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLSv1.2</td>
<td>ECDHE</td>
<td>AES-128-GCM</td>
<td>SHA-256</td>
<td>51.500%</td>
</tr>
<tr>
<td>TLSv1</td>
<td>ECDHE</td>
<td>RC4</td>
<td>SHA-1</td>
<td>29.225%</td>
</tr>
<tr>
<td>TLSv1</td>
<td>RSA</td>
<td>RC4</td>
<td>SHA-1</td>
<td>14.403%</td>
</tr>
<tr>
<td>TLSv1.2</td>
<td>ECDHE</td>
<td>AES-128</td>
<td>SHA-1</td>
<td>1.586%</td>
</tr>
<tr>
<td>TLSv1.2</td>
<td>RSA</td>
<td>RC4</td>
<td>SHA-1</td>
<td>1.147%</td>
</tr>
<tr>
<td>TLSv1</td>
<td>ECDHE</td>
<td>AES-128</td>
<td>SHA-1</td>
<td>0.999%</td>
</tr>
<tr>
<td>TLSv1.1</td>
<td>ECDHE</td>
<td>RC4</td>
<td>SHA-1</td>
<td>0.723%</td>
</tr>
<tr>
<td>TLSv1.2</td>
<td>RSA</td>
<td>AES-128-GCM</td>
<td>SHA-256</td>
<td>0.203%</td>
</tr>
<tr>
<td>SSLv3</td>
<td>RSA</td>
<td>RC4</td>
<td>SHA-1</td>
<td>0.060%</td>
</tr>
<tr>
<td>TLSv1.2</td>
<td>ECDHE</td>
<td>RC4</td>
<td>SHA-1</td>
<td>0.060%</td>
</tr>
<tr>
<td>TLSv1</td>
<td>RSA</td>
<td>AES-128</td>
<td>SHA-1</td>
<td>0.050%</td>
</tr>
<tr>
<td>TLSv1.1</td>
<td>RSA</td>
<td>RC4</td>
<td>SHA-1</td>
<td>0.024%</td>
</tr>
<tr>
<td>TLSv1.1</td>
<td>ECDHE</td>
<td>AES-128</td>
<td>SHA-1</td>
<td>0.011%</td>
</tr>
<tr>
<td>TLSv1.1</td>
<td>ECDHE</td>
<td>AES-256</td>
<td>SHA-1</td>
<td>0.004%</td>
</tr>
<tr>
<td>TLSv1.2</td>
<td>RSA</td>
<td>AES-256</td>
<td>SHA-1</td>
<td>0.003%</td>
</tr>
<tr>
<td>TLSv1.2</td>
<td>RSA</td>
<td>AES-128</td>
<td>SHA-1</td>
<td>0.001%</td>
</tr>
<tr>
<td>TLSv1</td>
<td>RSA</td>
<td>RC4</td>
<td>MD5</td>
<td>0.001%</td>
</tr>
</tbody>
</table>

Source:
"Neither Snow nor Rain not MITM... An Empirical Analysis of Email Delivery Security” Proceedings of the 2015 Internet Measurement Conference
Using DNSSEC and DANE to protect email
Three solutions to these attacks

<table>
<thead>
<tr>
<th>DNSSEC</th>
<th>DANE</th>
<th>Good TLS configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevents MX spoofing attacks</td>
<td>Authenticates receiving MTA</td>
<td>Prevents breaches in encryption</td>
</tr>
<tr>
<td></td>
<td>Prevents MITM downgrade attacks</td>
<td></td>
</tr>
</tbody>
</table>
DNSSEC deployment status

ccTLD DNSSEC Status on 2018-10-29

Typical signing rates:
- 100% in some new gTLDs
- ~50-60% in a few EU countries (NO, SE, NL, CZ)
- ~1% or less in most big developed countries
- Sweden: 49%

(Source: ISOC + DNSSEC Deployment Report, October 2018)
DNSSEC validation rates

Global average ~15%
(mostly thanks to Google’s public DNS service)

Nordics: 75-90%
Central Europe: 20-30%
USA: 23%
Swedish: 74%

(Source: APNIC Labs, November 2018)
What is DANE?

• DANE (RFC 6698) defines a new record type in DNS: the **TLSA record**
• Can be used to securely authenticate TLS certificates for any service and protocol:
  • By specifying constraints on acceptable trust anchors (CAs) and/or on own certificates
  • By allowing self-signed certificates to be explicitly permitted and verified
• **Uses DNSSEC as a trust anchor**
  • And also as a data security mechanism
• DANE is used in conjunction with SMTP & TLS to fully secure mail delivery
• DANE addresses vulnerabilities discussed earlier:
  • **Authenticates presented certificates** using DNSSEC signed TLSA record
  • **Prevents downgrade attacks** by making encryption mandatory for the domain (the presence of a TLSA record implies «encrypt or stop»)
Anatomy of a TLSA record

The record is associated to the service responding on a specific hostname, port and transport protocol. More than one record is possible.

Certificate usage:
0 = Trust anchor, PKI valid
1 = Host, PKI valid
2 = Trust anchor, no PKI validation
3 = Host, no PKI validation

Selector:
0 = Certificate
1 = Public key

Matching type:
0 = Full
1 = SHA-256
2 = SHA-512
Normal STARTTLS negotiation with DANE

DNS resolver

MX rcpt.com?

MX 5 mx.rcpt.com

TLSA _25._tcp.mx.rcpt.com?

TLSA 3 1 1 AC3BD7C0...

EHLO sender.com

250 STARTTLS

STARTTLS

Sending MTA

DANE

Certificate for rcpt.com

OK

ENCRIPTED TRAFFIC

Receiving MTA
MITM STARTTLS negotiation with DANE

DNS resolver

MX rcpt.com?

MX 5 mx.rcpt.com

TLSA _25._tcp.mx.rcpt.com?

TLSA 3 1 1 AC3BD7C0...

EHLO sender.com

Sending MTA

STARTTLS

DANE

FAIL

Certificate for attacker.com

Receiving MTA

250 STARTTLS

Attacker’s MTA
MITM downgrade attack with DANE

- **DNS resolver**
  - MX rcpt.com ?
  - TLSA _25._tcp.mx.rcpt.com ?

- **Sending MTA**
  - EHLO sender.com
  - TLSA 3 1 1 AC3BD7C0...
  - DANE FAIL

- **Receiving MTA**
  - 250 rcpt.com

- **Attacker's MTA**

---

- Sending MTA
- Receiving MTA
DANE adoption trend

- Number of domains having TLSA records
  - Numbers still tiny (~50k)
  - Other sources say ~300k for email

  Growth ~20%/yr

(Source: Verisign Labs, May 2018)
DNSSEC and DANE adoption in email
TES tool scan on top 1000 global web domains, May 2017

**DNSSEC**
- Deployed by 14 domains
- 1.8% of domains having email
- 2.3% of domains supporting TLS

**DANE**
- Deployed by 3 domains
- 0.3% of domains having email
- 0.4% of domains supporting TLS

The three lonely heroes: comcast.net, web.de and gmx.net
«DANE light»: MTA-STS

- Similar goals to DANE
- Policy published via HTTP
  - Requires MTAs to implement an HTTP client
- Trust on first use (less secure)
- Based on WebPKI
  - Relies on Certificate Authorities
  - No self-signed certs
- Deployment can coexist with DANE (but only if you use CA certificates)

- Also work ongoing on a reporting mechanism (TLSRPT)
  - Works with DANE or STS

*MTA-STS is officially only recommended as a temporary first step if you cannot or do not yet use DANE*
What can you do?
What can you do with DNSSEC and DANE?

Now

• Make sure your MTA uses a resolver with DNSSEC validation enabled
• Turn on DANE validation on outgoing email flows
• Bounce email that fails DANE validation (or at least try)

Tomorrow

• Deploy DNSSEC on all your production domains (if you didn’t already)
• Publish TLSA records for your own MTA’s certificates
• Ensure you know how to roll them over

In the very long term: turn off cleartext
(e.g. when we will all be using IPv6)
Thank you!

For further information:
https://tesmail.org/

Stay Open.