SMTP Transport Security: Past, Present, Future

Viktor Dukhovni
2015/10/20
Atlanta
Attendees Reminder:

What occurs in a M³AAWG meeting cannot be shared outside the membership

• Blogging, tweeting, posting is NOT allowed EXCEPT for referencing or citing the specific content on official M³AAWG public sites, which can be reposted or used in articles. The official sites are: www.m3aawg.org/DM3Z, www.Twitter.com/maawg, www.Facebook.com/maawg, https://www.facebook.com/groups/maawg/

• Respect M³AAWG anonymity: No publishing people or company names, except as cited on the official M³AAWG channels listed above

• No use of Wireshark or similar products on the M³AAWG network

• No photography - No video - No audio recording

• Any exception requires written permission from the Executive Director and may require permission from the session members

• All meeting attendees must wear and have their M³AAWG badge visible at all times during the meeting

• Please silence all electronic devices; be courteous to those listening to the presentations

• DO NOT LEAVE YOUR BELONGINGS UNATTENDED. Be aware and cautious at all times

Treat all attendees respectfully in and out of sessions. No less will be tolerated.

Please review our meeting Conduct Policy at http://www.m3aawg.org/page/m3aawg-conduct-policy

For questions, please contact Jerry Upton at: jerry.upton@m3aawg.org
Reminders for Our Worldwide Friends

*All meeting content is confidential: No photos, no video, no recording.*

*See staff with questions.*

L’ensemble du contenu de la réunion est confidentiel : les photos, vidéos et enregistrements sont interdits. Pour toute question, demandez conseil au personnel.

Todo el contenido de la reunión es confidencial: No está permitido sacar fotografías ni grabar vídeo o audio. Consulte con el personal si tiene alguna pregunta.

Der gesamte Inhalt des Meetings ist vertraulich: Keine Fotos, kein Video, keine Tonaufzeichnung. Bei Fragen wenden Sie sich an die Mitarbeiter.

会議の内容はすべて機密扱いです。写真やビデオの撮影、録音は禁止されています。質問がある方は、スタッフまでご連絡ください。

所有会 议内容均为保密信息：禁止拍照、录像、录音。如有疑问，请咨询职员。

회의에서 다루는 모든 내용은 기밀입니다. 사 진 및 동영상 촬영과 녹음은 금지됩니다. 질문이 있으시면 직원에게 문의해 주십시오.
PUBLIC INTERNET

GOOGLE CLOUD

GFE = Google Front End Server
GFE = Google Front End Server
SSL Added and removed here!
Traffic in clear text here.
Simple origins

- SMTP: RFC821, Aug 1982
- POP: RFC918, Oct 1984
- POP2: RFC937, Feb 1985
- **MX records**: RFC974, Jan 1986
- IMAP2: RFC1064, Jul 1988
- POP3: RFC1081, Nov 1988
Beyond username+password

- POP3: RFC1460, Jun 1993 (adds APOP)
- IMAP4: RFC1730, Dec 1994
- IMAP AUTH: RFC1731, Dec 1994
- POP3 AUTH: RFC1734, Dec 1994
Securing the transport

- DH patent expires Apr 1997
- RSA patent expires Sep 2000
- SUBMIT: RFC2476 Dec 1998
- TLS 1.0: RFC 2246 Jan 1999
- STARTTLS: RFC2487 Jan 1999
- AUTH: RFC2554 Mar 1999
- Widely implemented by end of 2000
Incremental progress

- AUTH, TLS and STARTTLS: 2006–2011
- Name checks in TLS: RFC6125, Mar 2011
- (Fuss over a citizen named Ed, Jun 2013)
- Prohibit RC4: RFC7465, Feb 2015
- Deprecate SSL 3.0, RFC7568, Jun 2015
- TLS 1.3: draft-ietf-tls13, Q2 2016?
New directions

- DANE: RFC6698, Aug 2012
- DANE SMTP: RFC 7671 and 7672, Oct 2015
- UTA drafts: email-tls-cert, deep
- DANE client auth draft?
- End-to-end encryption?
Multiple Security Models

• Mandatory MUA to Server TLS
  • DNS SRV for SUBMIT, POP, IMAP: RFC6186, Mar 2011
• Mandatory TLS for MTAs
• Islands of security: EMiG
• Opportunistic TLS for MTAs
• Opportunistic DANE TLS for MTAs
• Mandatory DANE TLS for MTAs
MUA to Server Security

- Simplest TLS use case
- Replace STARTTLS with implicit TLS?
- Use SRVID certificates?
- Security latching ala DEEP?
- Zeroconf ala RFC6186 via SRV records?
  - One time leap of faith?
  - Ongoing with DNSSEC?
Mandatory TLS for MTAs

- Variable security properties
- Poor scalability
- Weak or fragile peer name checks
- Not a feasible default policy
- UTA draft for cert checks and hosting?
Islands of Security

- Out of band ad-hoc TLS downgrade hardening
- Non-scalable
- Tried by "Email Made in Germany" (EMiG) consortium
- Mail to/from outside left unprotected
- EMiG announced DANE support by end 2015
- Let's not repeat this approach
Opportunistic TLS for MTAs

- Works well as a default policy
- 80% of messages from Gmail to other providers.
- Can we get to universal deployment?
- Vulnerable to man-in-the-middle downgrade
- Not widely understood

https://www.google.com/transparencyreport/saferemail/
Using Opportunistic TLS

- Upgrade from cleartext, not fallback from encryption (see RFC7435)
  - Don't expect (or bemoan lack of) valid certs

- Avoid silly downgrades, cleartext is not stronger
  - Accept untrusted certs, expired certs, certs with deprecated signature algorithms, ...
  - Accept weak ciphers while needed to interoperate
  - Disable SSL 2.0, SSL 3.0, EXPORT & 1DES
Advanced Opportunistic TLS

• Support server-side session tickets
• Implement client session caches (that work through load-balancers)
• Support ECDHE with sensible curves
• Configure adequate DHE parameters
• Avoid "exotic" cipher suites
  MD5, SRP, PSK, aDSS, kECDH, kDH, SEED, IDEA, RC2, RC5
Opportunistic DANE TLS

- RFC 6698, RFC 7671 and RFC 7672
- Domain publishes signed MX RRset
- MX host operator publishes signed A/AAAA records
- Two operating models
  - Per-server (End-Entity) TLSA records
  - Shared-issuer (Trust-Anchor) TLSA records
End-Entity TLSA records

- MX host operator publishes TLSA records
  `_25._tcp.mx.example.net. IN TLSA 3 1 1 server-key-digest`
  `_25._tcp.mx.example.org. IN TLSA 3 1 1 server-key-digest`

- Single certificate, no need for SNI
- No surprise expiration
- Key rotation requires prior DNS update
  `_25._tcp.mx.example.net. IN TLSA 3 1 1 current-key-digest`
  `_25._tcp.mx.example.net. IN TLSA 3 1 1 planned-key-digest`

- Then deploy new keys
Trust Anchor TLSA records

- CA operator publishes TLSA records
  
  _dane.example.net. IN TLSA 2 0 1 ca-cert-digest
  
- Servers publish CNAME records once:
  
  _25._tcp.mx1.example.net. IN CNAME _dane.example.net.
  
  _25._tcp.mx2.example.net. IN CNAME _dane.example.net.
  
- CA coordinates TLSA updates for cert rotation

- Server cert replacements with no DNS changes

- Expiration and name checks back in scope

- Can self-issue certificates for client domains!
Opportunistic DANE TLS

- Requires DNSSEC
- No CA "bundles"
- Downgrade resistant
- Scalable policy management
- Scalable TLS virtual hosting
- Scales beyond "islands of security"
Mandatory DANE TLS

- Require peer domain to publish TLSA RRs
- Much easier to deploy and manage
- Works with 3rd party hosting
DANE TLS adoption

- 7000+ domains
- 24 "prominent enough" for Google's report

- conjur.com.br
- lrz.de
- debian.org
- mypst.com.br
- posteo.de
- eu.org
- registro.br
- ruhr-uni-bochum.de
- freebsd.org
- societe.com
- tum.de
- ietf.org
- t-2.com
- unitymedia.de
- isc.org
- bayern.de
- lepartidegauche.fr
- openssl.org
- bund.de
- t-2.net
- samba.org
- jpberlin.de
- xs4all.nl
- torproject.org

- Large fraction in Germany, most "small"
- EMiG providers announced upcoming support
DANE implementation timeline

- Postfix DANE support, 2014
- Adopted by Exim, 2015
- RFC 7671 and 7672, Oct 15th
- Planned in OpenSSL, 2016
- More TLS toolkits?
- More MTAs?
- More providers?
Email TLS Certs

- Consistent cert checks for POP, IMAP and Submission
- Recommends SRV-ID altnames (CAs would have to start issuing these)
- Work-around for secure indirection w/o DANE
Deployable Enhanced Email Privacy

• DEEP: IMAP, POP and Submission privacy
• Assurance levels for email accounts
• Implicit TLS not STARTTLS (port 465)
• High assurance: Mandatory authenticated TLS
• No assurance: Opportunistic TLS
• Security latching (similar to HSTS)
• New CLNT command reports status to servers
• Certificate checks per email-tls-certs
End-to-end encryption?

- DANE WG experimental drafts publish key bindings for each user in DNS
- Proposed UTA WG "addrquery" draft uses SMTP extension
- Phillip Hallam Baker's CryptoMesh
- Real interest in key publication standards?
- Are any of the proposed approaches sound?
- Is E2E viable in the face of spam, malware, and usability requirements?
Questions?
Follow-up?

ietf-dane@dukhovni.org
rfc7435
rfc7671
rfc7672
draft-moore-email-addrquery
draft-hallambaker-cryptomesh