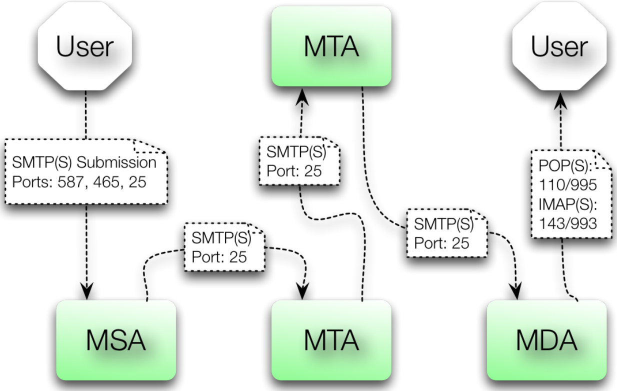
The State of Transport Security in the E-Mail Ecosystem

(Fast-forward edition)

RWC16 – Wilfried Mayer, **Aaron Zauner**, Martin Schmiedecker, Markus Huber

Background

E-Mail Flow

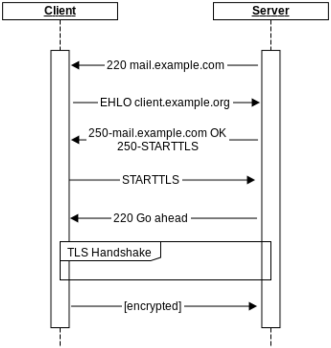


Background

Port	TLS	Protocol	Usage
25	STARTTLS	SMTP	Transmission
110	STARTTLS	POP3	Retrieval
143	STARTTLS	IMAP	Retrieval
465	Implicit	SMTPS	Submission
587	STARTTLS	SMTP	Submission
993	Implicit	IMAPS	Retrieval
995	Implicit	POP3S	Retrieval

Background

STARTTLS



Client

Server

220 mail.example.com

EHLO client.example.org

250-mail.example.com OK
250-STARTTLS

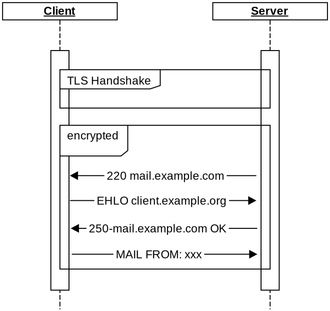
STARTTLS

220 Go ahead

TLS Handshake

[encrypted]

Implicit TLS



Client

Server

TLS Handshake

encrypted

220 mail.example.com

EHLO client.example.org

250-mail.example.com OK

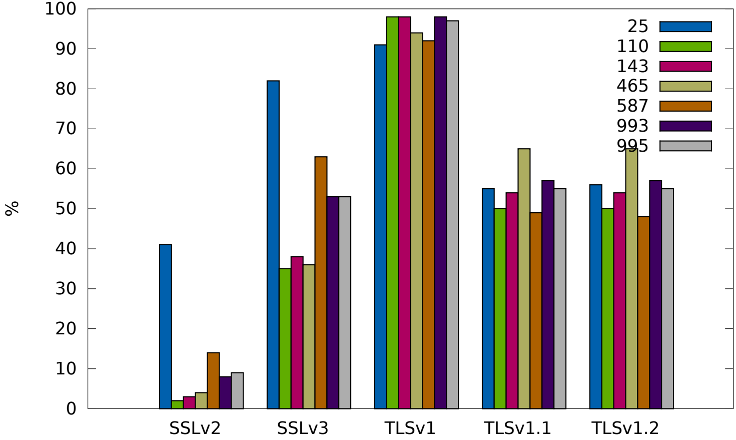
MAIL FROM: xxx

Results

Data Overview

- 20,270,768 scans conducted
- 18,381,936 valid reponses
- 7 TCP ports, 5 TLS versions
- $\sim$10 billion TLS handshakes
    - Combinatorial explosion - protocols, ports, ciphersuites and SSL/TLS versions
- 90% rejected — 8% accepted — 2% error
- April to August 2015

Results



%
100
90
80
70
60
50
40
30
20
10
0
SSLv2
SSLv3
TLSv1
TLSv1.1
TLSv1.2
25
110
143
465
587
993
995

Results

Protocol Version Support

Only	25	465	587	Retrieval
SSLv2 and SSLv3	0.2%	0.0%	0.0%	0.1%
TLSv1.1 and TLSv1.2	0.1%	0.0%	0.5%	0.1%
TLSv1 upwards	8%	45%	18%	32–37%

Results

Key-exchange security
Diffie-Hellman - DH(E):

- Large amount of 512bit DH primes in SMTP (**EXPORT**!)
- DH group size below or equal to 1024 bit is very common in all protocols

Elliptic Curve Diffie-Hellman - ECDH(E):

- SMTP: 99% use `secp256r1` curve
- POP/IMAP: about 70% use `secp384r1` cuve

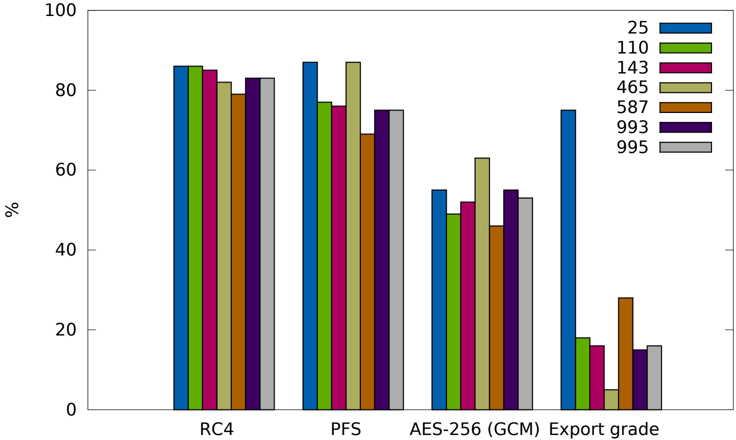
Results

Key-exchange security: common primes

- SMTP: a 512 bit prime used by 64%, a 1024 bit prime used by 69% (Postfix)
- 512 bit Postfix prime:

  ```
  0x00883f00affc0c8ab835cde5c20f55d
  f063f1607bfce1335e41c1e03f3ab17f6
  635063673e10d73eb4eb468c4050e691a
  56e0145dec9b11f6454fad9ab4f70ba5b
  ```

Results


100
80
60
40
20
0
%
25
110
143
465
587
993
995
RC4
PFS
AES-256 (GCM)
Export grade

Results

X.509 Certificates (cont.)

- 55%+ self-signed (or malformed)
- 99% of leafs use RSA
- Most SMTP(S) leafs and intermediates above 1024bit RSA (most 2k)
- Less than 10% use 4096bit RSA public keys
- SHA1 Fingerprint: `b16c...6e24` was provided on 85,635 IPs in 2 different /16 IP ranges

Name	Key Size	IPs
Parallels Panel - Parallels	2048	306,852
imap.example.com - IMAP server	1024	261,741
Automatic...POP3 SSL key - Courier Mail Server	1024	87,246
Automatic...IMAP SSL key - Courier Mail Server	1024	83,976
Plesk - Parallels	2048	68,930
localhost.localdomain - SomeOrganizationalUnit	1024	26,248
localhost - Dovecot mail server	2048	13,134
plesk - Plesk - SWsoft, Inc.	2048	14,207

All Results

`http://arxiv.org/abs/1510.08646`

Mitigation

Solid server configurations & awareness

- `bettercrypto.org`
- Mozilla Server TLS Security guide

  `https://wiki.mozilla.org/Security/Server_Side_TLS`
- RFC 7457 Summarizing Known Attacks on TLS and DTLS
- RFC 7525 Recommendations for Secure Use of TLS and DTLS
- Educating administrators, managers and operational people

Mitigation

New efforts in IETF and beyond

- DEEP (Deployable Enhanced Email Privacy) - similar to how HSTS works for HTTPS (MUA to Server)
- Let’s Encrypt!
- `draft-ietf-uta-email-tls-certs-05`: Identity verification for SMTP/POP/IMAP/ManageSieve updates various RFCs
- IETF works on a new OpenPGP spec

Mitigation - MTA to MTA

SMTP-STS (”Strict Transport Security”)
Pro:

- Good feedback Loop to detect active MITM
- Might work well for large ISPs/ESPs and protect at least this mail volume

Mitigation - MTA to MTA

SMTP-STS (”Strict Transport Security”)
Con:

- Engineered by & only built for large Mail hosting Companies
- Issues with Threat Model & Deployment at Scale
  `https://github.com/mrisher/smtp-sts/issues/1`
- Somewhat depends on DNSSEC
- Out-of-band authentication via Webserver and ‘.well-known‘ URL

Mitigation - MTA to MTA

Working on in-band verification/pinning solution for MTA to MTA security

- We need operator feedback
- We need active testing
- We still have some open issues (MX indirection, MTA specific cert handling,..) & need to write a proper Internet Draft