State of Transport Security in the E-Mail Ecosystem at Large

Aaron Zauner

IETF93 Prague, Security Area Open Meeting - 23/07/2015

Overview

Results

Conclusion

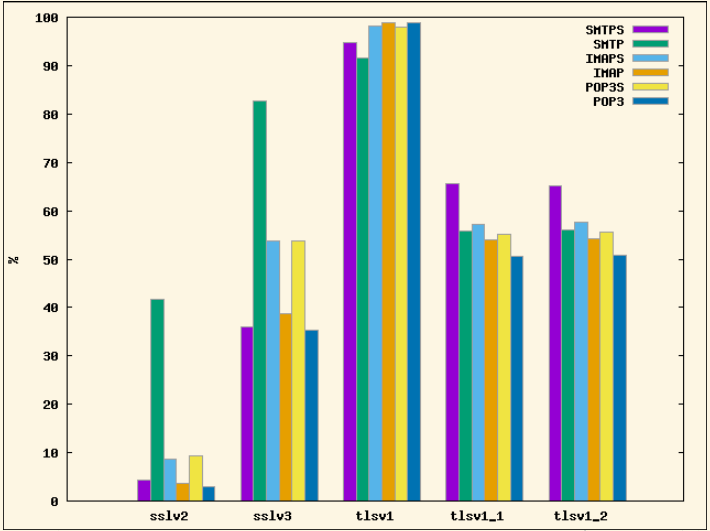
Context

- Joined SBA-Research in Janurary to help with an ongoing Internet-wide scanning project
- We've conducted scans on e-mail related ports over the last couple of months
- Currently digging through collected data and writing papers

Targets and Methods

- SMTP(S), POP3(S), IMAP(S) and Legacy Ports
- `masscan` and `sslyze` with a queueing framework built around it
- Delay between handshakes in `sslyze` added
    - some POP/IMAP daemons are easily DoSed
- Runs spanning months (roughly from April to June)
- About 9.2 billon TLS handshakes with `sslyze`
- Multiple `masscan` runs for banners/certs
- triggered `dovecot` bug (CVE-2015-3420) :)
    - initially discovered and investigated/reported upstream by Hanno Boeck

Protocol Support



RC4

	Accepting RC4	Not accepting RC4
SMTPS	82,27	17,73
SMTP	86,27	13,73
IMAPS	83,36	16,64
IMAP	85,71	14,29
POP3S	83,74	16,26
POP3	86,51	13,49

Table : RC4 Cipher Support Percentage

AUTH PLAIN offered by hosts

SMTP (25)

- 917,536 - AUTH PLAIN, no STARTTLS support
- 1,722,387 - AUTH PLAIN & STARTTLS

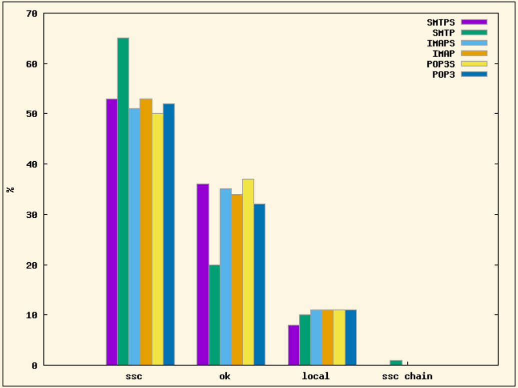
IMAP (143)

- 211,962 - AUTH PLAIN, no STARTTLS support
- 3,243,632 - AUTH PLAIN & STARTTLS

POP3 (110)

- 225,341 - AUTH PLAIN, no STARTTLS support
- 3,391,525 AUTH PLAIN & STARTTLS

Certificates



ssc: signed certificate, ok: CA signed, local: unable to get local issuer certificate, ssc chain: self signed certificate in certificate chain (Mozilla Truststore)

Certificates (cont.)

SMTP and SMTPS

- Almost all leafs >= 1024 bit RSA (most 2048)
- Same for intermediates (fewer than 200 with less than 1024 bit RSA)

POP3(S) and IMAP(S)

- Very similar results, a few more low-bit leaf and intermediates.

Weak ciphers and Anon-DH

SMTP (STARTTLS)

- RC2-CBC-MD5 - 40.9% accept (26.5% prefer!)
- IDEA-CBC-MD5 - 14.4% accept

SMTPS

- Anon-DH suites: about 12% acceptance

POP(S)/IMAP(S)

- Nothing too exciting, ask me about details if you're interested

Key-exchange

DH(E)

- Large number of 512bit DH primes in SMTP
- Sigificant amount of DH group size =< 1024 in all studied protocols

ECDH(E)

- Group size: most use 256, some 384, very few 521 throughout studied protocols

Common Primes

- Apache prime (Adrian et al 'Weak-DH' paper) not used
- mod_ssl prime: some users, very few

more on this topic TBD

Weak Keys

Analyzed 40,268,806 collected certificates. Rather unspecacular:

Fast-GCD (Heninger et al. "Mining P's & Q's", algo. by djb)

- 30,757,242 RSA moduli
- 2,354,090 uniques
- 456 GCDs found

Debian Weak-Keys (CVE-2008-0166)

- Compared to **`openssl-blacklist`** package
- A single (1) match

Conclusion

- First to conduct such a detailed study for E-Mail
  - A lot of issues with transport security in the e-mail ecosystem
  - Results are pretty much what we've expected beforehand
  - We'll publish all collected datasets (soon-ish)
- More studies, analysis and papers forthcoming
- We have tons of additional data, if you have specific questions write us!

Thanks for your patience. Are there any questions?

Point of contact: abuse@sba-research.org