# 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

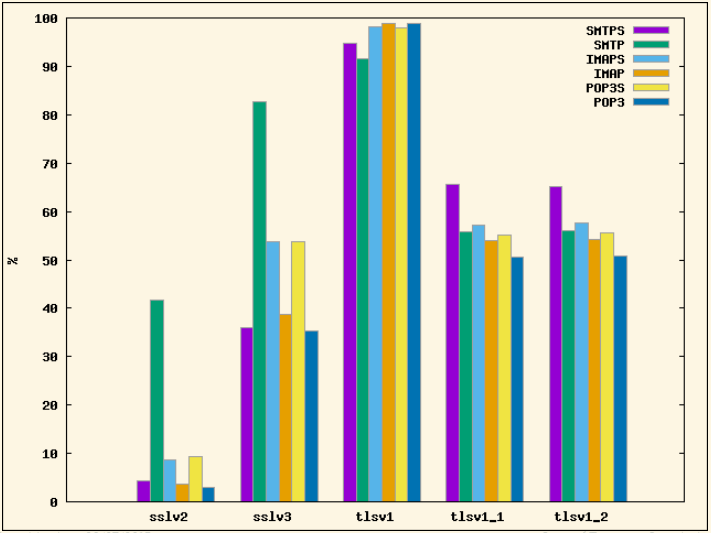
# Context

- 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) - AUTH PLAIN

- 917,536 do not offer STARTTLS
- 1,722,387 offer STARTTLS

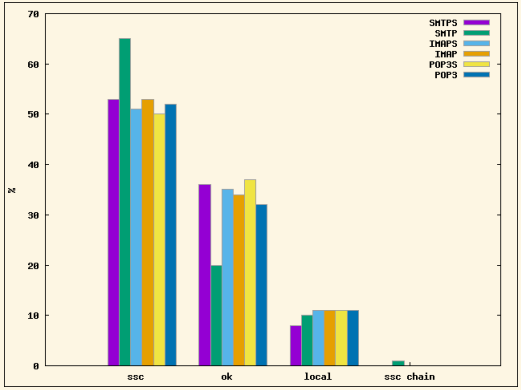
## IMAP (143) - AUTH PLAIN

- 211,962 do not offer STARTTLS
- 3,243,632 offer STARTTLS

## POP3 (110) - AUTH PLAIN

- 225,341 do not offer STLS
- 3,391,525 offer STLS

# Certificates




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

# 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

# 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
- Pretty much what we expected - no big surprises in the results
- A lot of transport security in the e-mail ecosystem
- More studies and analysis upcoming
- ..as are publications

Thanks for your patience. Are there any questions?