Verifying SMTP TLS with DANE

Jan-Pieter Cornet <johnpc@xs4all.net>

https://johnpc.home.xs4all.nl/dane/

One Conference, October 2, 2018.

XS4ALL

First Class Internet

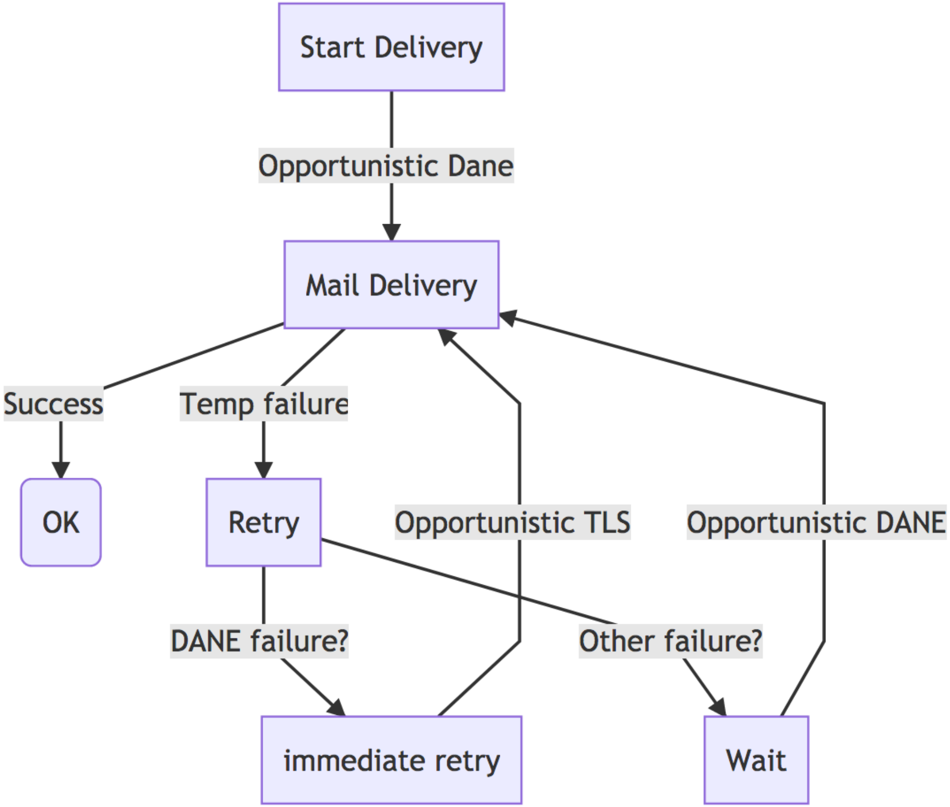
About XS4ALL

- Internet since ’93
- Focus on privacy and security, ease of use
  - Slightly rebellious
- Targeted at power-users
- I’m postmaster/CERT team

DANE at XS4ALL

- Publish TLSA records with DNSsec for over a year
- Started validating DANE on SMTP end of august 2018.
  - with cloudmark Gateway
  - … using soft-fail.

DANE “softfail”



danefail.org

- Add list of strict-DANE domains
  - (our own, havedane.net, various friendly parties)
- Add danefail list as non-DANE for all deliveries

Logging!

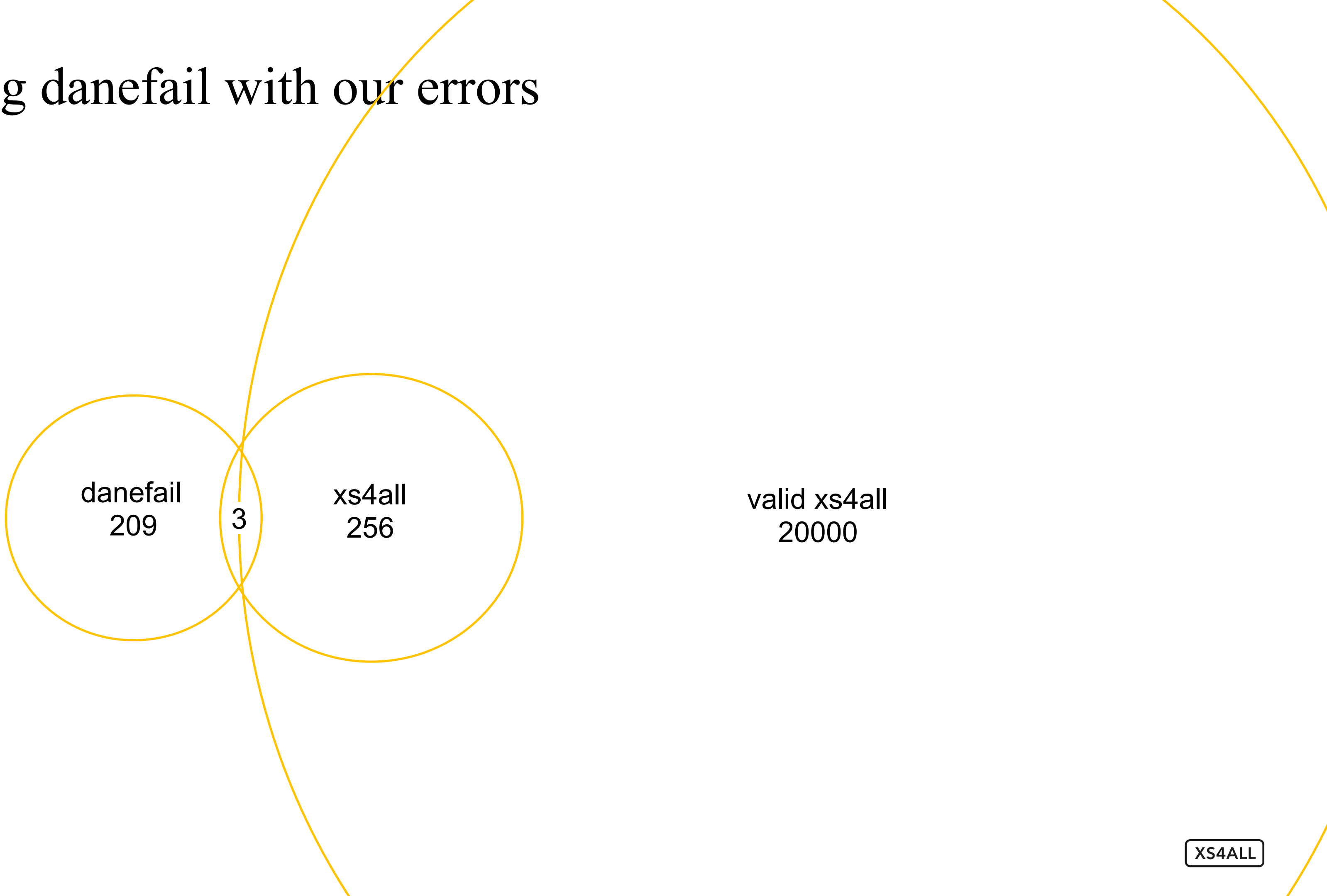
```
logline: to=example@gmail.com, mode=dane opportunistic, dane="Skip (Insecure
host information)", tls=TLSv1.2:ECDHE-RSA-AES128-GCM-SHA256, tlsvalid="0
(ok)", relay=gmail-smtp-in.l.google.com [108.177.119.27], dsn=250

logline: to=example@xs4all.nl, mode=dane strict, dane="Verify (Secure TLSA RRs
found)", tls=TLSv1.2:ECDHE-RSA-AES256-GCM-SHA384, tlsvalid="0 (ok)",
relay=mx1.xs4all.nl [194.109.24.132], dsn=250
```

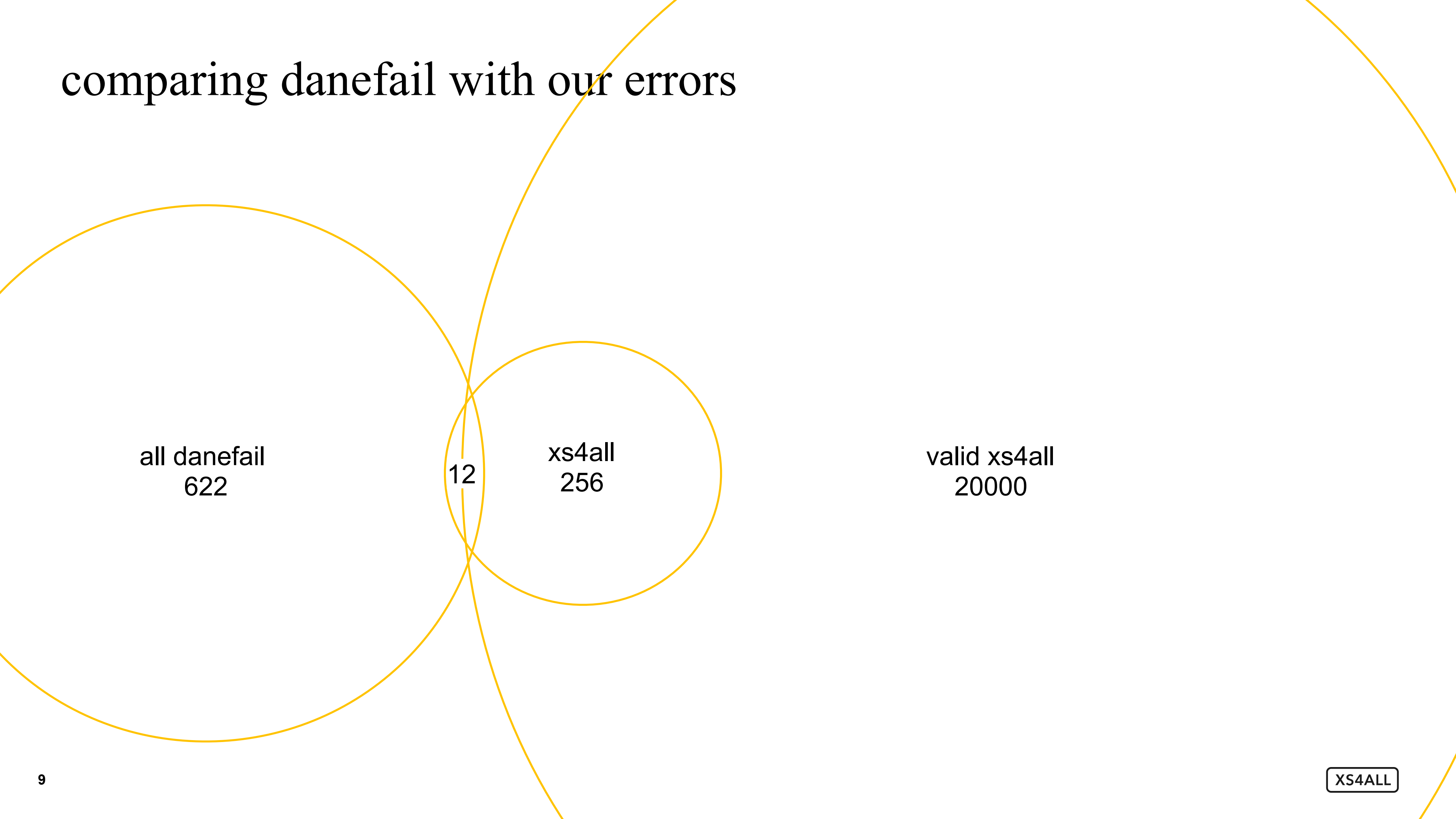
DANE related errors

- Certificate mismatch
- DNSSEC problems
- No STARTTLS
- Implementation bugs

comparing danefail with our errors

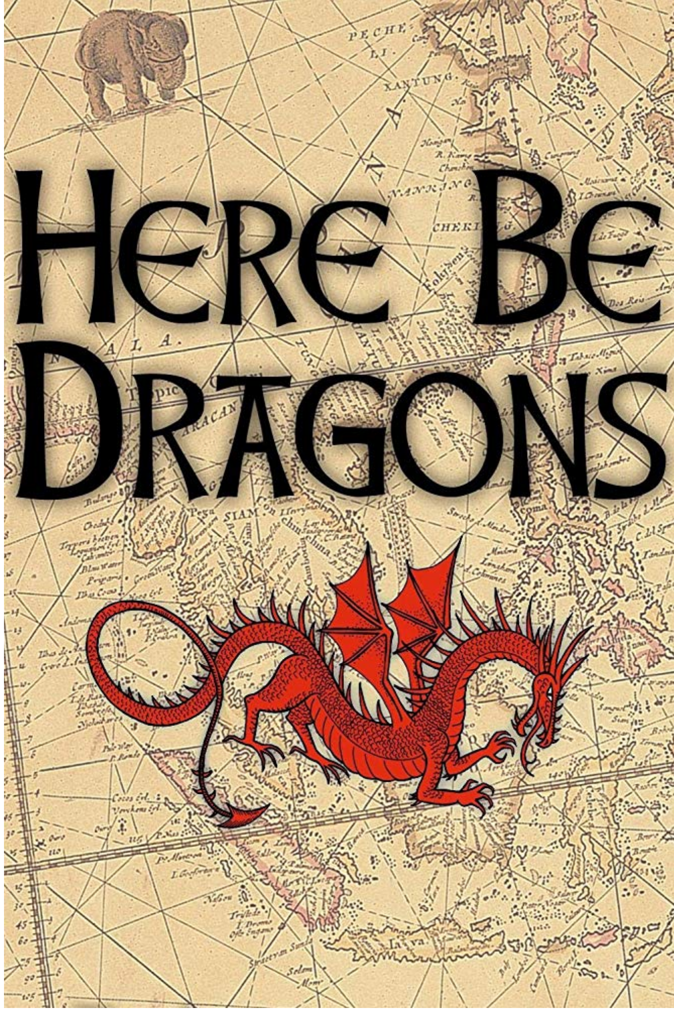


comparing danefail with our errors



lessons learned

- Watch out when you’re the first verifying DANE in a new area.
- Use either soft-fail
    - or monitor your logs faster than temp failures get rejected
- New software may have surprises



XS4ALL

turning on full DANE verification

- Need to work around/fix implementation bugs
- Add failing domains to danefail list.
- automate searching for more failures in logfiles.
  - report to receiver using RFC8460 SMTP TLS reporting?
- approx November 1, 2018.
- MTA-STS RFC8461?