Rates of HTTPS misconfiguration *vs* DNSSEC misconfiguration

Peter Thomassen <peter@desec.io>

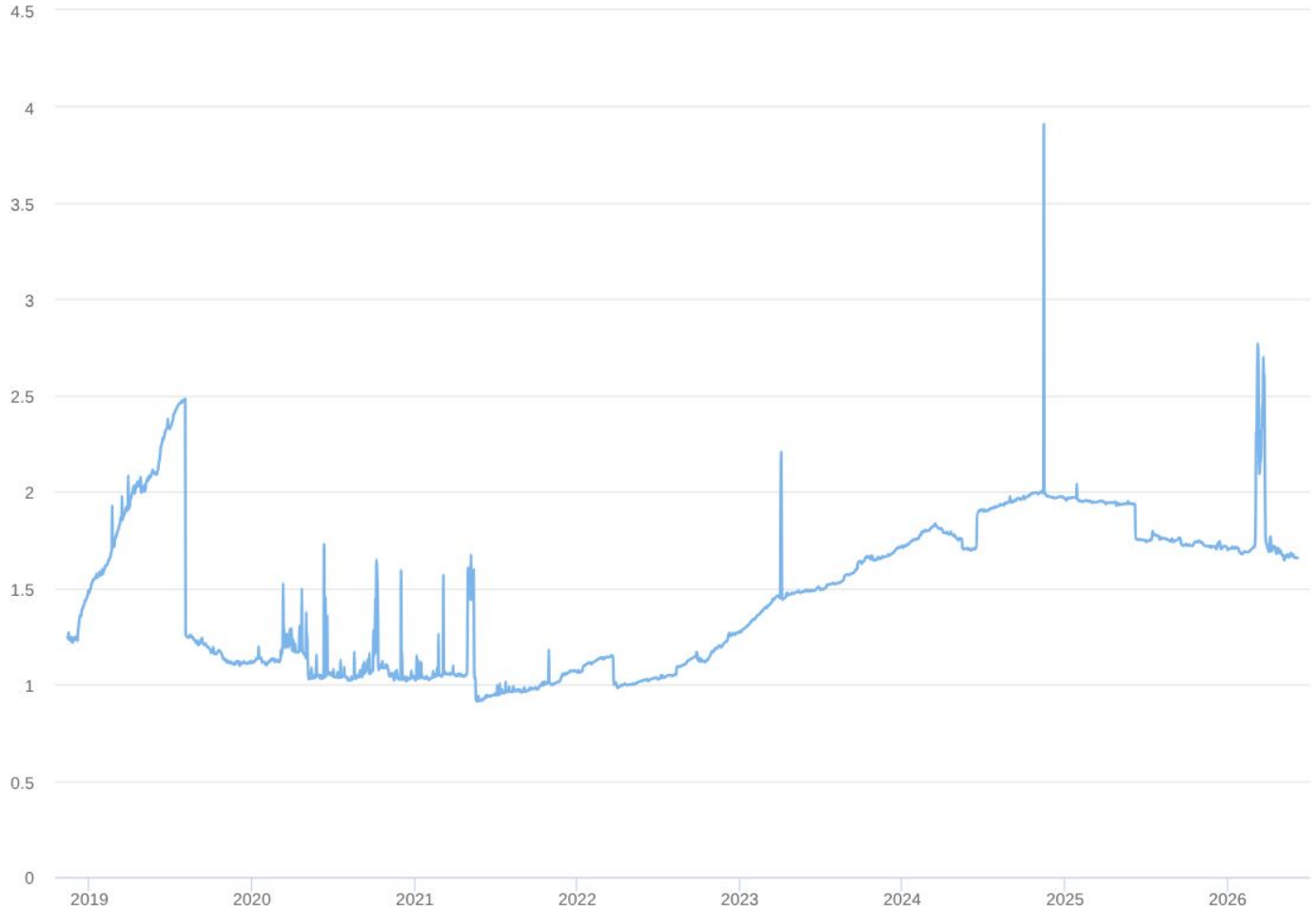
ICANN 86 DNSSEC Workshop – June 8, 2026

ICANN

This work is supported by the ICANN Grant Program

deSEC

The following graph shows the percentage of observed zones with a DNSKEY RRset that is failing to validate.



https://stats.dnssec-tools.org/#/?top=dane&trend_tab=1

deSEC

DNSSEC is error-prone. How much?

- 1–2% of DNSSEC-enabled domains
- Many possible reasons:
  - DS RRset points to non-existing keys only
  - Wrong signatures (operator failure: key confusion, …)
  - Expired signatures
  - Missing signatures
  - …

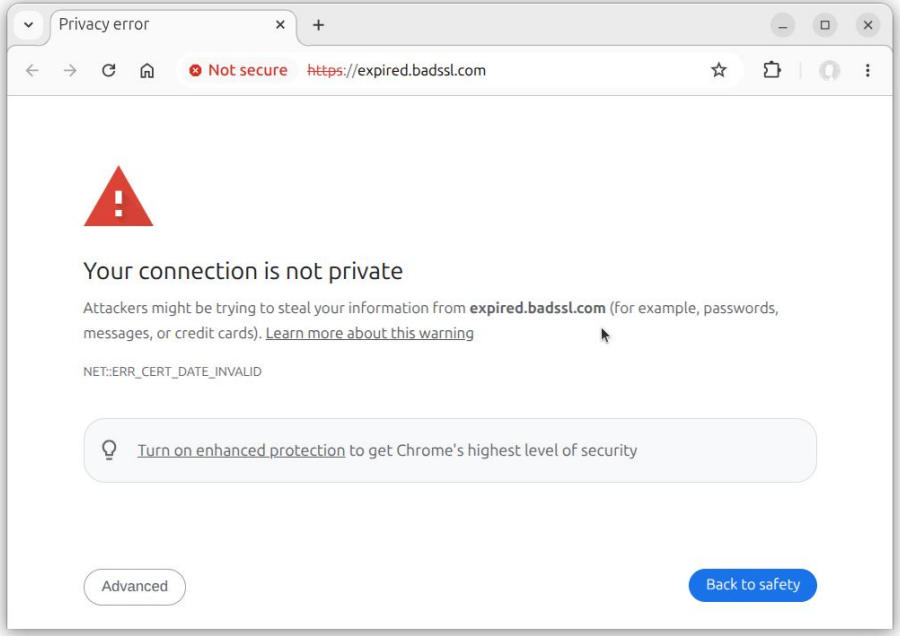
```
$ dig @8.8.8.8 dnssec-failed.org

; <<>> DiG 9.18.39-0ubuntu0.24.04.3-Ubuntu <<>> @8.8.8.8 dnssec-failed.org
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 31432
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
; EDE: 9 (DNSKEY Missing): (No DNSKEY matches DS RRs of dnssec-failed.org)
;; QUESTION SECTION:
;dnssec-failed.org.             IN      A
```

HTTPS is error-prone. How much?

- ?–?% of HTTPS-enabled domains
- Many possible reasons:
  - Wrong domain name in certificate
  - Intermediate certificates missing from handshake
  - Unknown CA
  - Expired certificate
  - Unsupported cipher
  - Wrong key/certificate pinned
  - …
- Used to be more common!



Inputs

- Sample: CrUX Top Million (via https://github.com/zakird/crux-top-lists)

  "Websites are ranked by completed pageloads (measured by First Contentful Paint) and aggregated by web origin. The dataset adheres as closely as possible to user-initiated pageloads (e.g., it excludes traffic from iframes)."

- Simulate real browser behavior by mixing in intermediates (via https://github.com/FiloSottile/intermediates)

  "a list of known unexpired, unrevoked intermediate certificates chaining to [...] the Mozilla Root Program. [...] useful to establish connections to misconfigured servers that fail to provide a full certificate chain but provide a valid, publicly trusted end-entity certificate. Some browsers implement similar strategies to successfully establish connections to these sites."

Measurement

For any domain on the CrUX list,

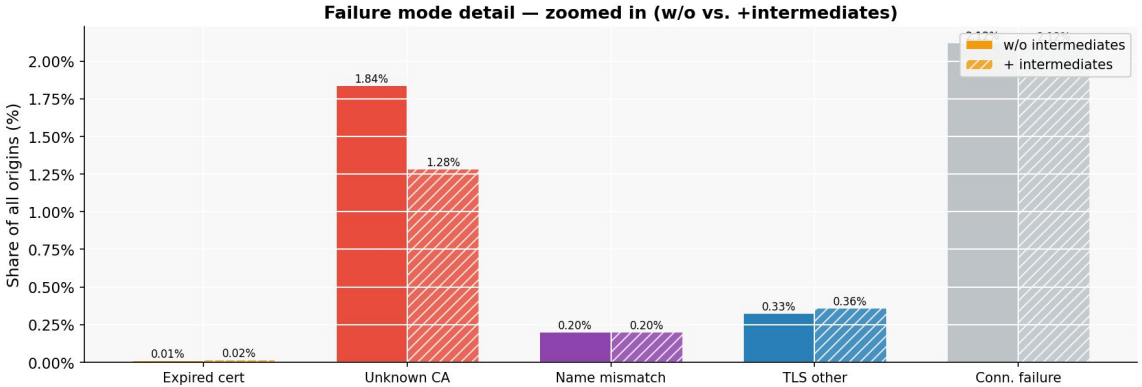
- perform TLS handshake on port 443
- record outcome (OK/expired/unkown_ca/name_mismatch/tls_other/conn_fail)

… both for OS trust store only, and with intermediates mixed in

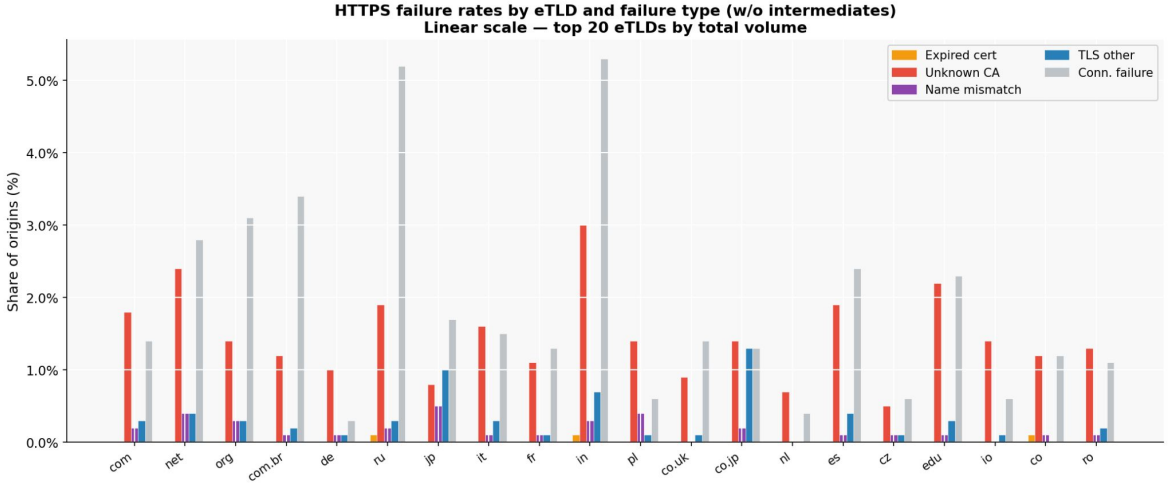
- Measurements conducted on April 29, 2026
- Aggregated by eTLD (effective TLD = public suffix)

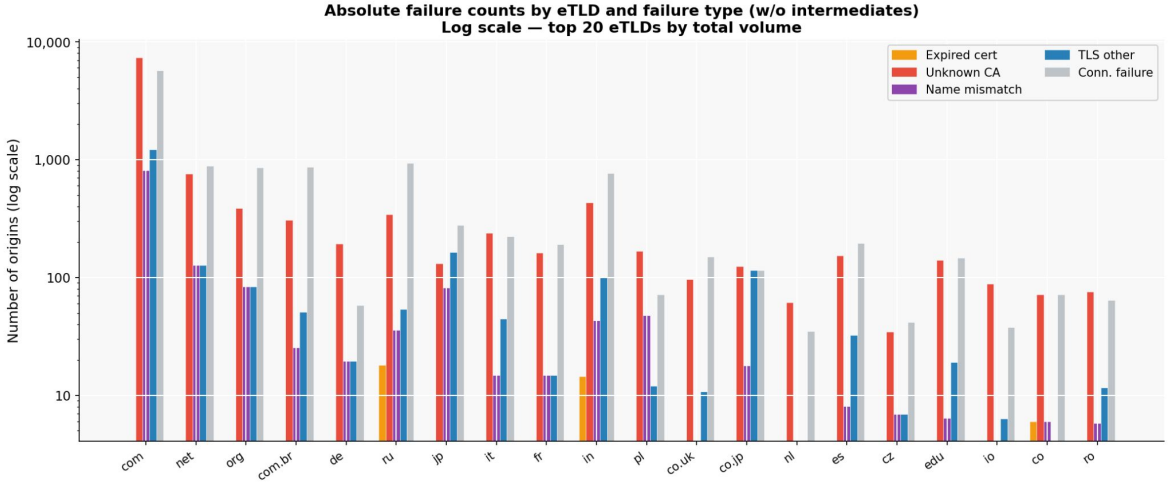
deSEC

HTTPS outcome distribution — top 1M CrUX origins

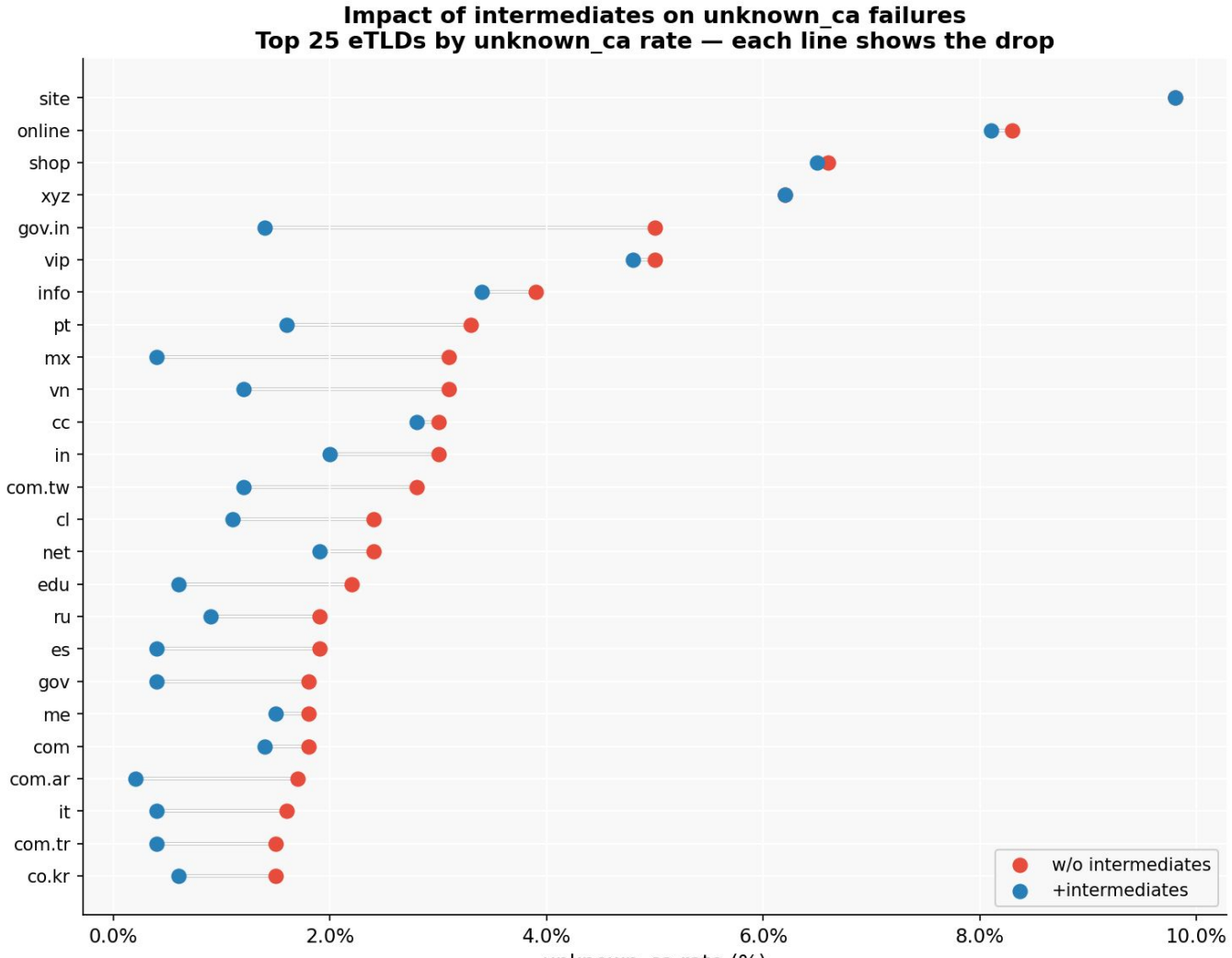


deSEC


HTTPS failure rates by eTLD and failure type (w/o intermediates)
Linear scale — top 20 eTLDs by total volume
Share of origins (%)
0.0%
1.0%
2.0%
3.0%
4.0%
5.0%
Expired cert
Unknown CA
Name mismatch
TLS other
Conn. failure
com
net
org
com.br
de
ru
jp
it
fr
in
pl
co.uk
co.jp
nl
es
cz
edu
io
co
ro

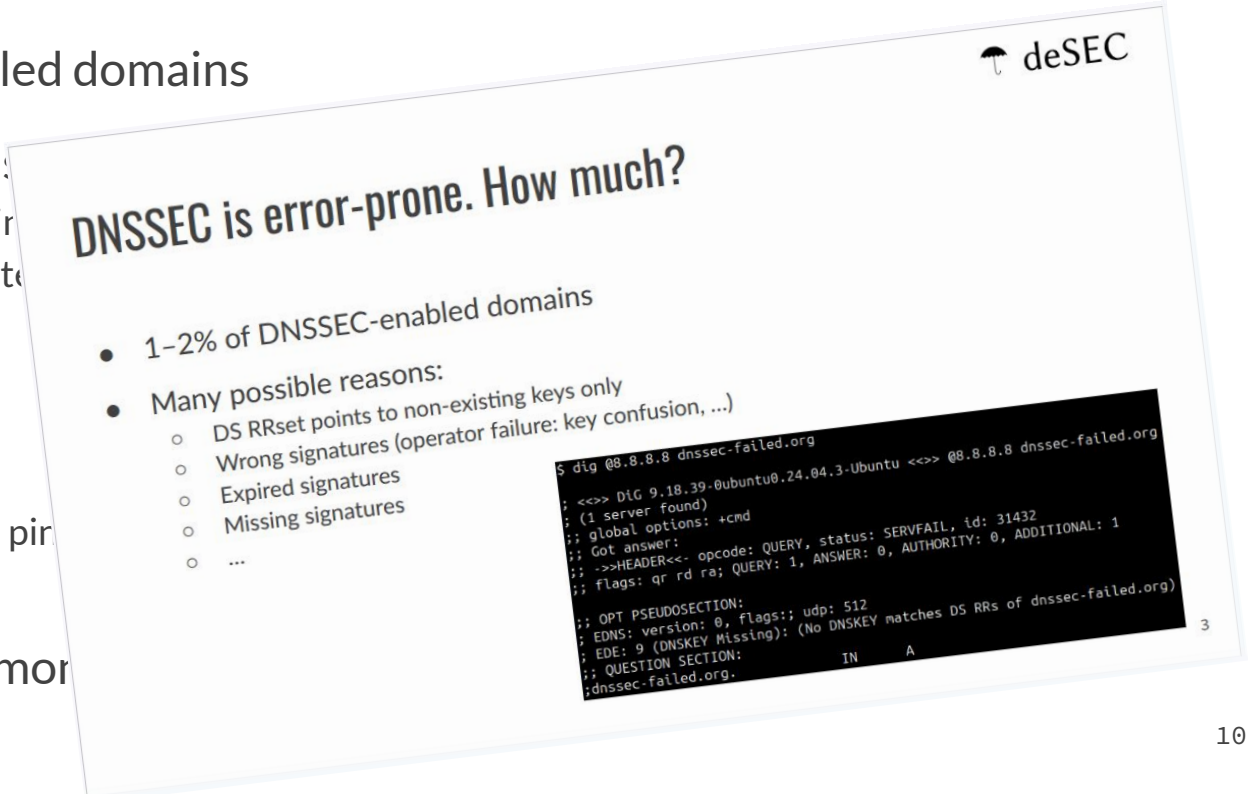

Absolute failure counts by eTLD and failure type (w/o intermediates)
Log scale — top 20 eTLDs by total volume
Number of origins (log scale)
10
100
1,000
10,000
Expired cert
Unknown CA
Name mismatch
TLS other
Conn. failure
com
net
org
com.br
de
ru
jp
it
fr
in
pl
co.uk
co.jp
nl
es
cz
edu
io
co
ro

deSEC


Impact of intermediates on unknown_ca failures
Top 25 eTLDs by unknown_ca rate — each line shows the drop
site
online
shop
xyz
gov.in
vip
info
pt
mx
vn
cc
in
com.tw
cl
net
edu
ru
es
gov
me
com
com.ar
it
com.tr
co.kr
0.0%
2.0%
4.0%
6.0%
8.0%
10.0%
w/o intermediates
+intermediates

HTTPS is error-prone. How much?

- 1–2% of HTTPS-enabled domains
- Many possible reasons:
  - Wrong domain name in
  - Intermediate certificate from handshake
  - Unknown CA
  - Expired certificate
  - Unsupported cipher
  - Wrong key/certificate pair
  - …
- Used to be more common



HTTPS ≠ DNSSEC

- Not making any claims about impact
- Not suggesting that a DNSSEC failure is like an HTTPS failure
  - DNSSEC misconfiguration in a TLD typically is like a CA or intermediate failing
- Adding data points to the discussion

Questions

- Is this useful?

If yes,

- Should there be stats over time?
  - Anyone dare to place a bet on automation impact?
- How to improve the measurement?