(Anecdotal) Analysis of DNSSEC Risk

Peter Thomassen <peter@desec.io>

ICANN78 – DNSSEC and Security Workshop
October 25, 2023

DNSSEC Operational Problems (actual & perceived)

– – –

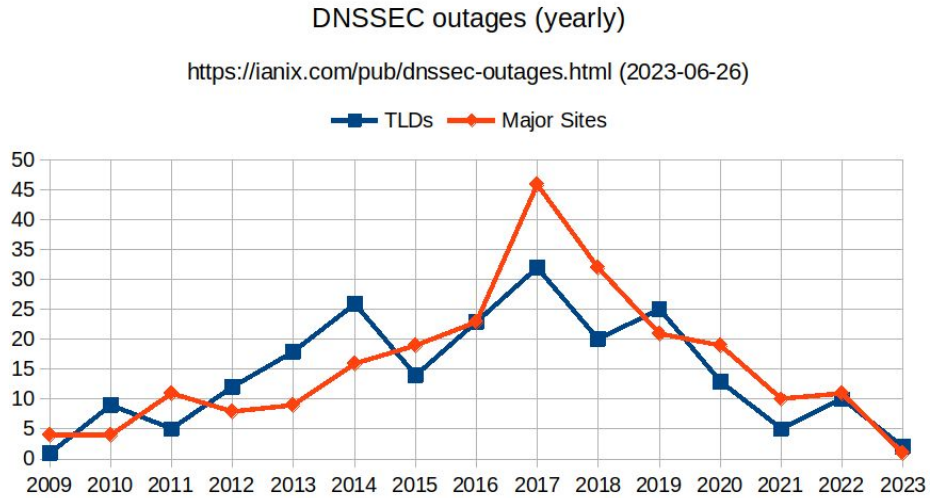
- Misconfigurations have led to outages
  - Frequently cited source: IANIX (https://ianix.com/pub/dnssec-outages.html)
  - Curated (using unknown criteria)
    → Grain of salt: **No statements on systematic errors in this talk!**
- Maintenance takes time
  - Depends very much on degree of automation
- Amplification attacks / DDoS
  - ATT has refused to implement DNSSEC for this reason
  - UTwente: not a problem when using suitable algorithm; consistent with (low) number of reports
- Tradeoff: client-side validation benefits ↔ latency
  - Might lead to delay for painting web pages etc. (depending on how it's done)

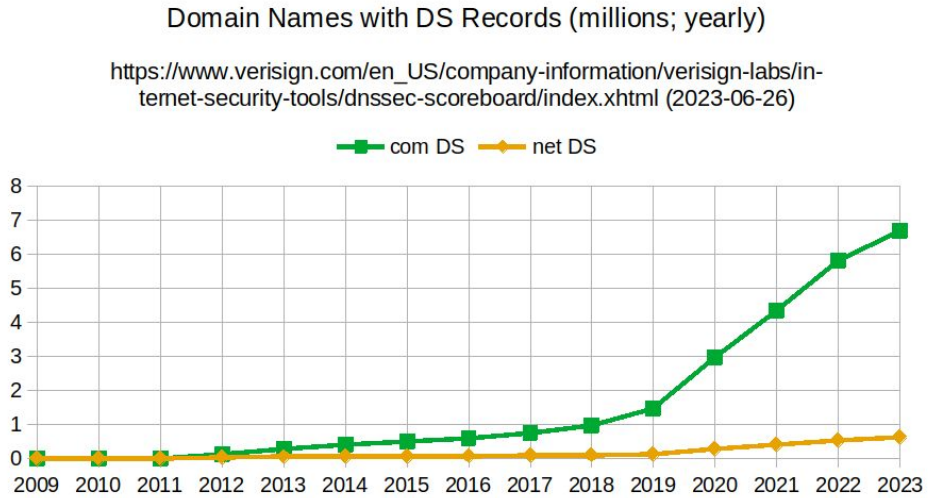
Misconfiguration Perils and Maintenance Pains

– – –

- Initially (> 6 years ago): **Manual signing, manual key maintenance**
- Today: **Tooling / native support available** for all of that
  - Includes automatic key rotation & algorithm rollover (incl. waiting for cache expiration etc.)
- Number of **deployments increasing**, number of **incidents decreasing**
  - risk = #incidents / #deployments → **risk decreasing**
- Automation greatly **reduces overhead**
  - deSEC hosts 27k zones, **all with fully automated DNSSEC operations → no overhead**
  - One issue remains: automation for setting DS records → see TechDay contribution
- Some things will always go wrong. But: **fixing the tooling, it's fixed for good**
  - Example: In 2021, Amazon Route 53's buggy DNSSEC implementation broke slack.com (fixed!)

DNSSEC Incidents vs. Deployment Size



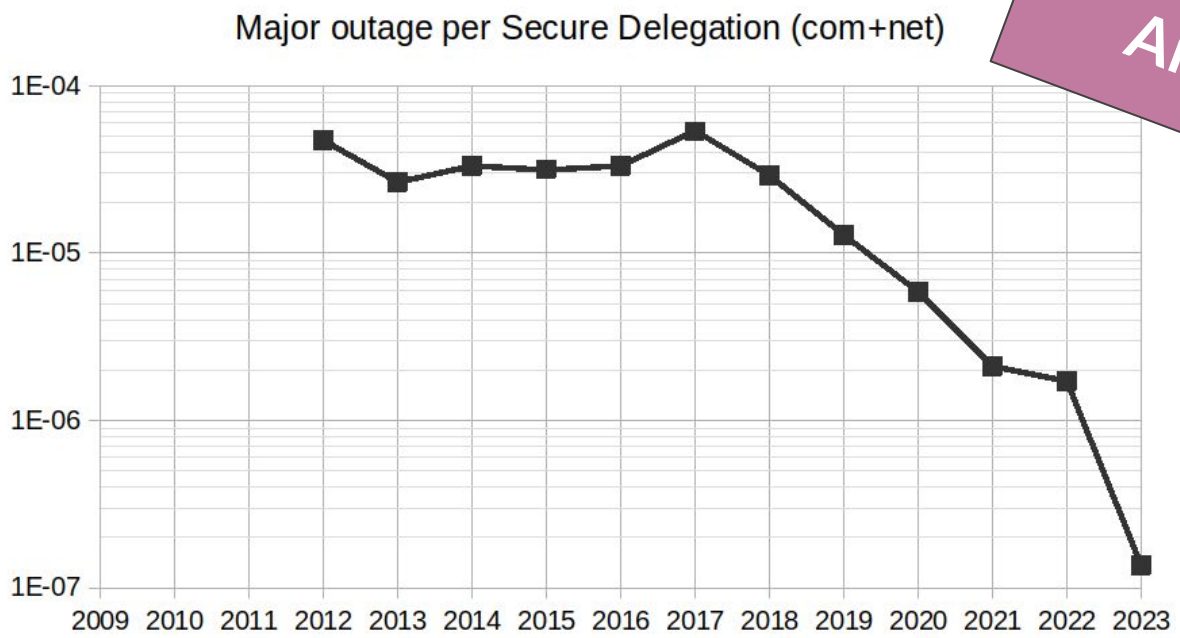


https://ianix.com/pub/dnssec-outages.html (anecdotal)

https://scoreboard.verisignlabs.com/

Signing rates: 8% (top 100), 16% (top 1000), 7% (global)

Estimated Deployment Risk of DNSSEC Decreased by ×50



Anecdotal

This is the ratio of the two previous diagrams.
(2023 numbers until June.) – Note: **logarithmic** scale!

Conclusions

- Tooling has much improved over past years
- Incidents haven't grown at same rate as deployment
- If the last years were acceptable, even more so now!

Opportunities for improvement:

- TTLs of DNSSEC-related RRs (in particular, DS)
  - Short TTLs needed for rollback (says Google at ICANN 75) and feasible (says ISC at OARC 41)
- Structured evaluation of DNSSEC-induced outages would be helpful

Thank you!

… also to our supporters:

Questions?

Dr. Peter Thomassen

peter@desec.io
peter.thomassen@securesystems.de