New Curves in DNSSEC

Ondřej Surý, CZ.NIC

SafeCurves(.cr.yp.to)

- Work by Daniel J. Bernstein and Tanja Lange
- Difference between security of:
  - Elliptic-Curve Cryptography (ECC)
  - Elliptic-Curve Discrete-Logarithm Problem (ECDLP) ← how to find a secret key from PK
- The ECDLP might be fine, but implementation might not:
  - Your implementation produces incorrect results for some rare curve points.
  - Your implementation leaks secret data when the input isn't a curve point.
  - Your implementation leaks secret data through branch timing.
  - Your implementation leaks secret data through cache timing.
- SafeCurves criteria are designed to ensure ECC security, not just ECDLP security

Edwards-curve Digital Signature Algorithm (EdDSA)

1. High-performance on a variety of platforms.
2. Does not require the use of a unique random number for each signature.
3. More resilient to side-channel attacks.
4. Small public keys (32 or 57 bytes) and signatures (64 or 114 bytes).
5. The formulas are "strongly unified", i.e., they are valid for all points on the curve, with no exceptions. This obviates the need for EdDSA to perform expensive point validation on untrusted public values.
6. Collision resilience, meaning that hash-function collisions do not break this system.

https://datatracker.ietf.org/doc/draft-irtf-cfrg-eddsa/

SafeCurves by CFRG

- Curve25519 → Ed25519
  - 2006 Daniel J. Bernstein
  - ~128-bit security target
- Curve448(-Goldilocks) → Ed448
  - 2014 Mike Hamburg
  - ~224-bit security target

RFC 7748

SafeCurves in DNSSEC

- draft-ietf-curdle-dnskey-ed25519
  - Adopted in CURDLE WG
    - Consensus for use in DNSSEC
  - In need of review
  - Waiting for draft-irtf-cfrg-eddsa
- draft-sury-dnskey-ed448
  - Might be adopted in CURDLE WG
    - No strong consensus for use in DNSSEC
- Future draft-<something>-kill-old-dnskey-algo
  - We need to start deprecating old DNSSEC algorithms

DNSSEC Algorithm flexibility

- ~Quick~ adoption by DNS server vendors
- Very slow adoption in real world deployments
  - Slow life cycles in Linux (and other) distributions
  - Even slower deployment (people still run 2012 distros)
  - Other reasons
- Workshop at DNS-OARC in Buenos Aires