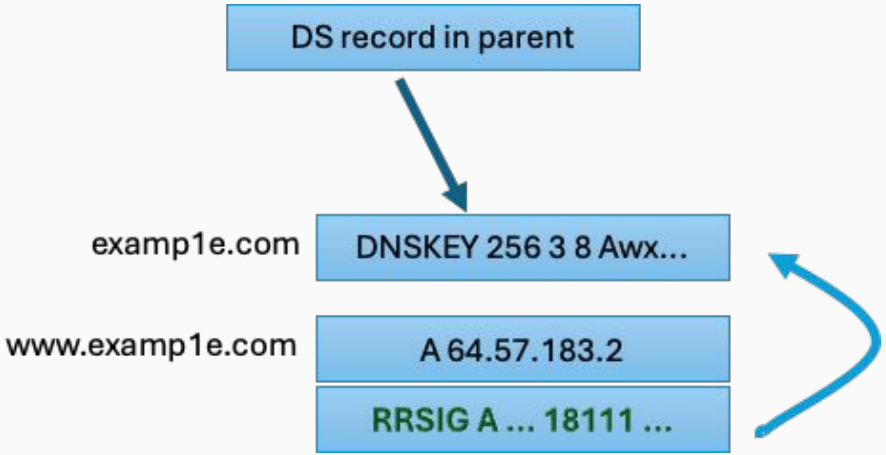
Two Trendy Ways to Hang Your DNS Cache

John Levine | ICANN 79 San Juan 🌴

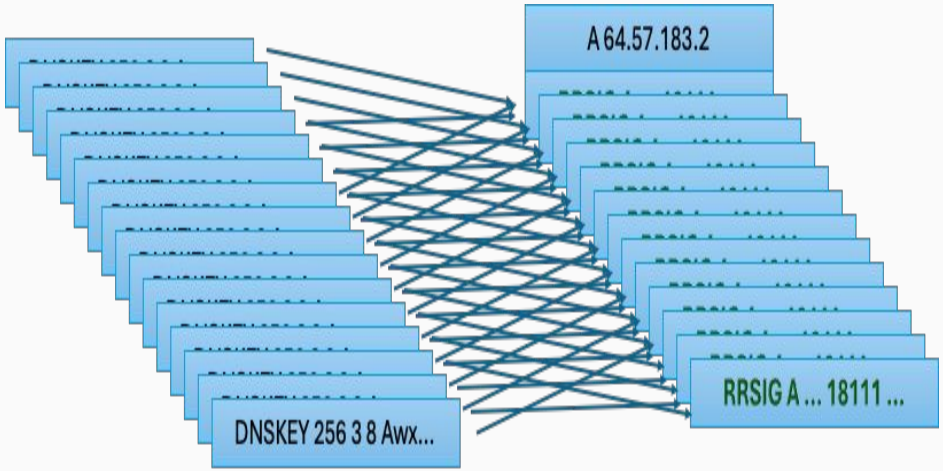
Keytrap

DNSSEC Signed Records



- DNSKEY has validation keys for RRSIGs
- Can be multiple DNSKEY and RRSIG for key roll
- RRSIG has ID number (18111) to find correct DNSKEY
- ID is 16-bit checksum of DNSKEY
- ID need not be unique
- Easy to make duplicate IDs

Keytrap



- 100 DNSKEY with ID 18111
- 100 RRSIG with ID 18111
- 100x100 = 10,000 validations
- Validation done in main thread of DNS cache, can hang it for minutes
- Oops

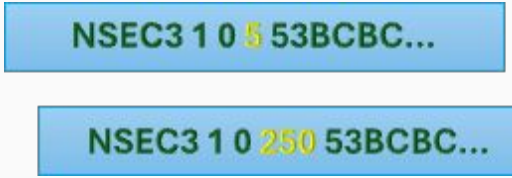
How bad is this?

- Possible since RFC 4034 in 2005, just discovered a few months ago
- Responsible disclosure, all major caches updated
- BIND: move validation to separate threads, limit work
- Unbound: suspend after 8 and try later
- No real zone has more than two colliding keys so give up after 5 or so
- There are many ways to craft DNS answers to do unreasonable work, e.g. CNAME loops. **This is just another one**.

NSEC3 Closest Encloser

Speaking of just another

- While fixing keytrap, ISC found another
- NSEC3 “closest encloser” to prove non-existence from name hashes
- Hash iteration count in the record
  - RFC 9276 says 1 iteration is plenty
- Make a zone with high iteration count NSEC3s
- Spray random queries at it
- Endless hashes to find encloser name



aa.bb.cc.dd.ee.ff.gg.hh.ii.jj.kk.ll.mm.examp1e.com
bb.cc.dd.ee.ff.gg.hh.ii.jj.kk.ll.mm.examp1e.com
cc.dd.ee.ff.gg.hh.ii.jj.kk.ll.mm.examp1e.com
dd.ee.ff.gg.hh.ii.jj.kk.ll.mm.examp1e.com
ee.ff.gg.hh.ii.jj.kk.ll.mm.examp1e.com
ff.gg.hh.ii.jj.kk.ll.mm.examp1e.com
...
examp1e.com

How bad is this?

- Possible since RFC 5155 in 2008, just discovered a few months ago
- Responsible disclosure, all major caches updated
- Same fixes, separate threads, limit iteration count, etc.

Tempest in a teapot?

- Pretty much
- Straightforward to fix
- The DNS has a lot of these

Two Trendy Ways to Hang Your DNS Cache

John Levine | ICANN 79 San Juan 🌴