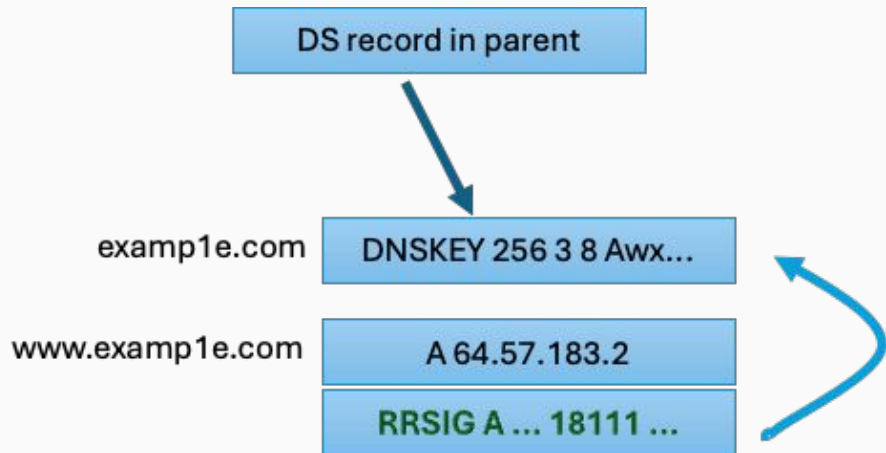


IDs in Collision or Keytrap, not so much

John Levine | ICANN 79 SSAC San Juan 🌴

DNSSEC Signed Records



- DNSKEY has validation keys for RRSIGs
- RRSIG has ID number to find correct DNSKEY
- ID is 16-bit checksum of DNSKEY
- Checksum is pretty lame

How common are duplicate IDs?

- Looked at every gTLD with a million names or more
- Looked at .SE and .NU that have a lot of signed names
- Total over 200,000,000, but most not signed
- Fetched DNSKEYs, computed and checked IDs

zone	size	serial
com	157508614	1708992020
net	12840911	1708905620
org	10800093	1708992392
info	3599182	1708991880
xyz	3302304	3000779938
online	3000132	1364146
top	2680697	1708993225
shop	2354816	1708996613
site	1524978	368496
store	1433654	300659
biz	1240243	1708991536

What did we find?

- In 200 million domains, 107 apparent collisions
- 86 are KSK and ZSK with same ID
- 20 pairs of ZSK, 1 of KSK with same ID

Coll	Not	Zone
0	0	app
0	0	biz
18	68	com
0	0	dev
0	0	info
0	10	net
2	2	nu
0	0	online
1	5	org
0	1	shop
0	0	site
0	0	store
0	0	top
0	0	xyz

Domains with duplicate IDs

a-holding.com. 256
affiliatemarketingstartup.com. 256
cinetoto.com. 256
cooneycompanies.com. 256
elviasmultiservices.com. 256
erkoportfoolio.com. 256
focusing-minds.com. 256
getshitdonedie.com. 256
gexperiments5.com. 256
natea-groupe.com. 256
nif4you.com. 256

pictures-talk.com. 256
shivarpanam.com. 256
thccleaningllc.com. 256
trinity-electric-llc.com. 256
unazuye.com. 256
wheelook.com. 256
xn--formsatelit-6gb.com. 256
cloudwerken.nu. 256
copperhill.nu. 257
liverec.org. 256

What did I find?

- A tiny handful of ID collisions
- All look accidental
- All were only two keys
- **No collisions of three or more**
- Don't need fancy mitigation, just stop when you see more than, say 5
- Couldn't count RRSIGs but I expect similar numbers

IDs in Collision or Keytrap, not so much

John Levine | ICANN 79 SSAC San Juan 🌴