DNSSEC Challenges for small DNS providers

John Levine

Standcore LLC

Regops Workshop, April 2016

Hi! I'm a small DNS provider

- Two servers
- One remote mirror
- Home brewed web console
- Automated scripts create zones
- Zones pushed to my servers with rsync
  - Mirror uses NOTIFY and AXFR

My customers

- Mail domains
- Hosted web domains
- Random people with mail or web other places
- Mix of mostly non-technical users
  - My church
  - My father
  - Friends from college
  - Ex-coworkers
  - The guy who wrote VisiCalc

My suppliers

- Tucows reseller, about half of the domains
- Various other registrars
  - Including other Tucows resellers
- Various TLDs (.ly .am …)
- Tucows hosted mail
- Various other web hosts

The easy part

- Create zone files, update remote reference hacks
- Sign them all
  - Create new KSK and ZSK for new zones
- Rsync them out to the servers
  - Give or take one server that still uses NOTIFY and AXFR
- Serve up all that DNSSECy goodness

The hard part

- Install DS or DNSKEY in parent zone

The easy part of the hard part

- Tucows has powerful reseller API
- Can manage all domains in my reseller account
- A little python script can do this:
  - Unlock a domain
  - Install the DS record
  - Re-lock it

The hard part of the hard part

- Users with other registrars
  - I'm their DNS operator, not their registrar
- Users with other Tucows resellers
  - Can't use API on other customers
- Random other TLDs
  - Some are helpful like .AM but it's all tedious

The score card

- Installed to my Tucows account customers: 122
- Installed by hand elsewhere: 2
- Not installed: 101

Solutions?

- It's a classic bootstrap problem
- Various drafts
- I really don't want one that requires that I collect passwords or other credentials.
  - They know they're delegating to my servers

OMG! No HSM! It's Insecure!

- Look at the real threat model
  - My server is physically fairly secure and has no unknown users
- These domains are not paypal.com
- Registrar accounts all use login/password