PayPal

DNSSEC EXPERIENCE

Bill Smith

March 2012

BACKGROUND

- How many domains do you have?
- We have
  - 1100+ registered domains (and counting)
  - 50+ actually active
  - Marketing creating random new domains with no oversight
- This includes such gems as:
  - Paypal-dostuffformoney.com
  - Operationfruitcake.com
  - PayPal-turn[s*][10|ten].[com|org|net|biz|ccTLD]

FOREGROUND

- Process (need one)
    - Move all parked domains to our registrar with redirects to some business site
    - What do do with .asia as an example?
- Internal process change
    - All domains start parked
    - No domain can change from parked unless process followed (right)
- After cleanup
    - Change our DNS infrastructure to move to dynamic zones
    - Add automation
    - One of the primary motivators for this was preparing for DNSSEC

DNSSEC

- What went well?
  - Overall very smooth
  - Phased rollout leaving critical domains towards the end
  - Plan rollout, some domains will need to be moved before others
- What went less well?
  - Lack of an consistent or standard way to upload DS keys
  - No consistency between the TLDs
  - DS key updates are entirely manual which is not flexible or scalable
- Any surprises?
  - Everyone wants to use DS keys
- What would we do differently?
  - Might separate signing systems from zone masters
  - Signing as a proxy in the middle
  - Wasn’t an option at the time, but is now (may change)

DNSSEC (CONT)

- How long did it take?
  - Eight Months
  - Generally very smooth
  - Little drama
  - Phased rollout essential
- Was it difficult?
  - Signing wasn't difficult
  - Changing DNS setup from static files to dynamic zone somewhat more so
  - Knew DNSSEC was coming and factored that in to infrastructure improvement making DNSSEC implementation easier
- Are we done?
  - In process of doing some of the same work with our in-addr.arpas, but for all forwards, we're done

FUTURE

- Challenge now is key rotation
- Set that up and start doing it
- Concern is less from a security perspective and more from an operational perspective
    - Do them rarely, no one will know how they are done
    - Our plan is to rotate three times a year to maintain operational proficiency
    - This will stress the "DS key upload" problem
    - Might induce enough upstream pain to encourage move towards an automated process

CONCLUSION

- Not as hard as we might have thought
- Planning is essential
- You won’t think of everything
- Start early
- Speak with your suppliers
- Do it now