Have a Strategy in Place
For Unexpected DNSSEC Events

Wes Hardaker
<wes.hardaker@parsons.com>

Overview

- Your Operational Panic Binder
- DNS Failure Strategies
- DNSSEC Failure Strategies
- Documenting Lessons Learned

Your Operational Panic Binder

- Good operators
  - Document Procedures
  - Document How-To
  - Document What-Ifs
  - Document Recoveries
  - Document Everything

Your Operational Panic Binder

- Good operators
  - Document Procedures
  - Document How-To
  - Document What-Ifs
  - Document Recoveries
  - Document Everything
- Bad operators...

Your Operational Panic Binder

- Good operators
  - Document Procedures
  - Document How-To
  - Document What-Ifs
  - Document Recoveries
  - Document Everything
- Bad operators
  - ***Panic***

Your Operational Panic Binder

- Good operators
  - Document Procedures
  - Document How-To
  - Document What-Ifs
  - Document Recoveries
  - Document Everything
- Bad operators
  - ***Panic***

(created by LOVETEESMUGS on Zazzle)

Your Operational **DNS** Panic Binder

- What goes in it?
- What problems can you foresee?
- What problems have you had?

Your Operational **DNS** Panic Binder

- Problems with your servers
  - One goes down
  - One is out of sync
- Problems with your network
  - A critical link goes down
  - A routing problem
- Problems with your parents
  - Out of sync data
- Problems with your children
  - They're under a DDOS attack

Your Operational **DNS** Panic Binder

- An example page: A slave server is out of sync
  1) SSH to slave.myzone.com using 192.0.2.5
  2) Run “rndc reload” as root
  3) dig @localhost myzone.com SOA
  4) Does it match the master? If yes, stop
  5) Run “service restart named”
  6) Dig @localhost myzone.com SOA
  7) Does it match the master? If yes, stop
  8) SSH to master.myzone.com using 192.0.2.1
  9) Run “service restart named”
  10) ...

Your Panic Binder With DNSSEC

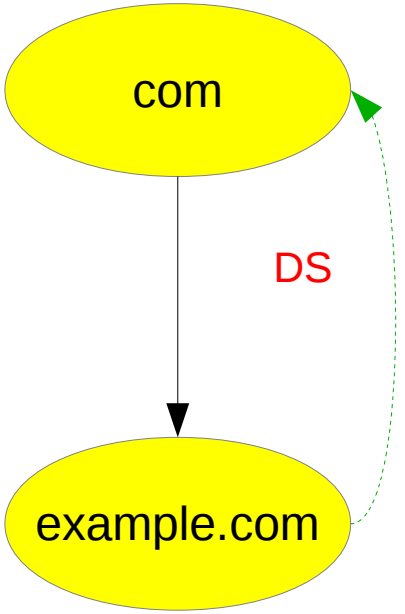
- You should have a Panic Binder!
  - If you do, does it contain potential DNSSEC problems?
- What does DNSSEC add to your binder?
  - A number of new things
  - Probably less than your binder already contains
  - Increases time-related problems
  - Increases the need for contact information
    - To Parents
    - To Children
  - Do you have canned responses for support staff?

DNSSEC Binder Materials

- DNSSEC Signature Expiration
  - How can you resign? fast?
  - How can you push out updates? fast?
  - Same as needing to update an A record fast
  - How long until all the caches are flushed?
    - How long are the TTLs?
- Are you testing for this failure?

DNSSEC Binder Materials

- Missing DS record
  - How to create a DS record
  - How to publish it to your parent
    - Website?
    - Admin request?
    - Submit via a DS key or a DNSKEY
  - How to get it from your client
- Are you testing for this?
  - Would you know if there **is** a problem?



DNSSEC Binder Materials

- DNSSEC Key Compromise
  - How do you generate new keys?
  - How do you put them in place?
  - How do you resign using the new ones?
  - How do you inform your parent of the new DS?
    - Do you have contact info?
  - How long will it take to propagate, given TTLs?
  - Is anyone using your key as a trust anchor?
    - How do you update their notion of your key?
  - Similar to a fast NS record change!
- Are you testing for mistake key changes?

DNSSEC Binder Materials

- Algorithm Issues
  - Unknown Algorithm with an important validator
    - Explain they need to upgrade?
    - Publish an additional DS record?
  - Algorithm Broken
    - What if ECDSA is broken?

DNSSEC/DANE Binder Materials
(Top 10 DANE/SMTP issues seen)

1) DANE and DNSSEC as a fashion statement
2) Failure to automate signing
3) Failure to update TLSA RRs **before** updating cert
4) Using DANE-TA(2) but not sending the CA in inside TLS
5) Unsupported certificate asage (using PKIX-TA or PKIX-EE)
6) Incorrect TLSA selector
7) Incorrect TLSA digest
8) Selective availability of STARTTLS
9) Firewalls that filter out TLSA queries
10) Broken nameservers
11) Partial Implementation

https://dane.sys4.de/

DNSSEC Binder Materials

- Contact Information
  - Parent or parent registar's contact information
    - Website
    - Phone number
    - Support email
  - Client information
    - Client DNS administrator information
    - Client Nameservers

DNSSEC Binder Materials

Discussion!

What else??

(created by LOVETEESMUGS on Zazzle)

Questions?

Wes Hardaker
<wes.hardaker@parsons.com>