Formal Benchmarking of Registries
Jay Daley .nz
ccTLD benchmarking today
Only 2048 bits will do

- Earlier this year published DNSSEC Practice Statement for consultation
- Recommended 1152 KSK length
- Complaints from community
  - “Most other TLDs using 2048 - so should we”
- Argued that 1152 is extremely secure
  - Well known cryptographer agreed with us
- Community not satisfied - perception issue
Changing environment

- New things keep going wrong
- New services appear from time to time
- People keep inventing new stuff
- The bar keeps rising higher!
Using benchmarking

- What are our peers doing?
  - how are we placed in relation to them?
- What is industry best practice?
  - how are we placed with regard to this best practice?
- What goals should we set?
  - how do we know they will be effective
- What should we be measuring?
- How do we demonstrate best practice to our community?
Lost in best practice acronyms

- Some are already used by registries
  - ITIL - IT service management
  - COBIT - Framework for control over IT
  - ISO 9000 - Quality framework
  - ISO 27000 - Information security
  - ISO 31000 - Risk management

- Nothing registry specific!
Levels of maturity

1. Repeatable
   - Home grown approach, little external reference, manual intervention in processes, intuitive

2. Defined
   - Automated, documented and communicated

3. Managed
   - Monitored, measured, incorporates some best practice

4. Optimised
   - Adopts all known best practice, “just works”

5. Advanced  (a new one just for us)
   - Advancing the field, delivering excellence
Possible elements 1

DNS
- name server placement / connectivity
- name server software
- name server performance
- name server capacity
- name server resilience
- zone file transfer
- dns monitoring
Some examples

DNS Monitoring

- Level 2. DSC or equivalent on each server
- Level 3. Central aggregation of logs
- Level 4. Every DNS query logged,
- Level 5. Developing expert tools to analyse

Name server software

- Level 4. 3 or more name server implementations. Actively involved in the development of some of these.
- Level 5. Custom written name server
Possible elements 2

- Registry
  - registry protocols
  - transaction performance
  - transaction capacity
  - registry system resilience
  - registrar connection management
  - availability checkers
  - IDN support
  - DNSSEC support
Possible elements 3

- **WHOIS**
  - rate limiting
  - access control (whitelists, blacklists)
  - features (flags, UTF-8)

- **Security**
  - security reviews (firewall, IDS, pen testing)
  - registrar interface security
  - support for registrant lock
Some more examples

Reviews

- Level 1. No reviews
- Level 4. Scheduled frequent external reviews of security, registry operations, IT management (e.g. COBIT, ITIL). Review results published to community.
- Level 5. Active in developing registry benchmarking

Registrar interface security

- Level 4. All connections from Registrars are from white-listed IP addresses, use client certificates and/or public key crypto signatures. All interfaces are penetration tested regularly.
Possible elements 4

Infrastructure
- database resilience (single master, multi-master with no transaction loss)
- Internet connectivity
- team specialisms

Services
- Registrar support (out of hours, online system)
- web site (documentation, statistics)
Metrics to measure

Each maturity level requires

1. Certain measurements to be taken
2. Minimum performance against those

For example:

Nameserver performance

- No more than X dropped queries, average of Y milliseconds for response

Security reviews

- X pen tests per year
One size does not fit all

- Not everyone is the same
- Set expected level appropriately for size
- Only the very biggest can aim for level 5 across the board
- Business priorities determine the goals
Who does it?

- Lots of work to set this up
- Needs testing in some registries
- Accredited consultants who can assess against model
  - Need to ensure quality in assessment
- Continual development
- Volunteers?
Any questions?

jay@nzrs.net.nz