DNSSEC in .nz

Jay Daley
2013
Current Position

- DNSSEC fully implemented
- Staged rollout May-Sep 2012
  - geek.nz as the first second level
  - Others including co.nz
  - Moderated second levels like govt.nz
- Second send of key signing ceremonies
- ~30 signed zones from ~520,000
Checklist

- DNSSEC Practice Statement
  - Key management policies
- Signing infrastructure (using HSMs)
- Software changes
- Rollout plan
- Side effects dealt with
  - Zone transfer time
  - Amplification attacks
DNSSEC Practice Statement (DPS)

- Community acceptance
  - Agreement with regulator
  - We publish DPS and consult community

- Verifies
  - We are meeting needs of our users
  - Technical scrutiny

- BUT .... Lots of problems!
  - Substantive issues follow
Problems with DPS

“KSK size too small”

- We chose 1152
- Some in community wanted 2048
  - “Everyone else does it”
  - “We should have the strongest possible”
  - “Why risk 1152?”
- Famous cryptographer defended 1152
  - Not enough for some
- We changed to 2048
Problems with DPS

“Must audit staff thoroughly”
- Criminal checks
- Financial checks
- Drug checks

We were only planning criminal
- “We trust you but what if you leave?”

Agreed to financial checks for new staff
Problems with DPS

◊ “Need Trusted Community Representatives (TCRs) like ICANN”
◊ “They provide independent audit”

◊ Our response
◊ More people to security vet
◊ Already have independent auditors
◊ ICANN method is security theatre

◊ We did not include TCRs
Problems with DPS

“Need full details of site security”
“Cannot trust if we do not know”

Our concerns
Too much information makes them a target

Final agreement
Specification for site security published
Protocol for site access included
Conclusion

öm Community engagement on DPS is vital
öm Some views will be irrational but must be accommodated
öm This is the community view after all
öm Lots of very useful feedback
öm Very useful process overall
Any questions?

jay@nzrs.net.nz