



DISI Update

Olaf Kolkman, Henk Uijterwaal & Daniel Karrenberg



Outline

DNSSEC status

DISI achievements since RIPE 45

Impact of signing on zone size; some measurements



DNSSEC status

- Documents in final state. Review is needed!
 - Some venom in the tail... still open issues.
- Q1 2004 for running code and proposed standard is optimistic but not unrealistic.
 - All depends on resolving open issues, final review in the WG, the IESG and funding of code development.
- DNSSEC will be based on new RR types:
 - DNSKEY, DNSSIG and NSEC
 - Same functionality as KEY, SIG, NSEC
 - Get used to these names.



Since RIPE 45

- Focus on the implementation of DNSSEC into the registry system
- Turned into a review, involving almost all engineering departments, of the reverse DNS setup.
- DNSSEC makes us look at
 - Server infrastructure review
Some results on later in this presentation
 - Review and redesign of the zonefile generation



DNSSEC, MARVIN and WHOIS

- Marvin (auto-inaddr@ripe.net) is the system that does zone file generation; updates WHOIS DB and zonefiles.
- We'd like to use one authoritative data source; the WHOIS DB
- Use the existing WHOIS DB authentication model for DNSSEC registration
 - As strong as the registration process is currently.
- Ease the creation of Domain objects.

- Overall plan presented in the services working group
 - Details to be discussed in the various RIPE working group



Since RIPE 45 (continued)

- IETF related work
 - Internet-Drafts
 - draft-ietf-dnsext-key-signing-flag is in IETF last call
 - Documenting Key management issues (with Gieben)
 - draft-kolkman-dnssec-key-ops-00.txt
 - We consider this one of the main tasks of this project; stable DNS operations and hence good operation procedures are of common interest.
 - Contributing to the process as co-chair of the DNSEXT working group
 - Interest is growing in DNSSEC key management issues; will (need to) find a place in the IETF.



Since RIPE 45 (even more)

- Software development,
 - Minor changes to key management software.
 - Distribution deferred until we get more experience.
 - Drop a mail if you are interested in alpha code.
- Net::DNS::SEC is being updated to reflect the typecode roll.
 - Has been posted to CPAN this week.
 - Tools depending on this library are showing up (e.g. on www.dnssec.net)



DNSSEC Training courses

Important aspects of DISI is raising awareness

- Since RIPE 45: May 17 Barcelona (16), June 3 Stockholm (15), July 18 Viena (25), August 18 Dubai (15).
- Planned: September 19 Amsterdam, October 10 Istanbul, October 28 Rome

Also see

- <http://www.ripe.net/cgi-bin/courselist.pl.cgi>
- Material available via <http://www.ripe.net/disi>



DNSSEC on ns.ripe.net

Empirical results for 1024bit keys

- Operational problems may occur if dnssec is not taken into account
 - e.g /var partition: the file space needed for our secondary zones grows from 500Mb to 5Gb when all zones are signed.
 - Sufficient memory on the server is important
- CPU load did not seem to be an issue (but the server in our setup was memory bound)

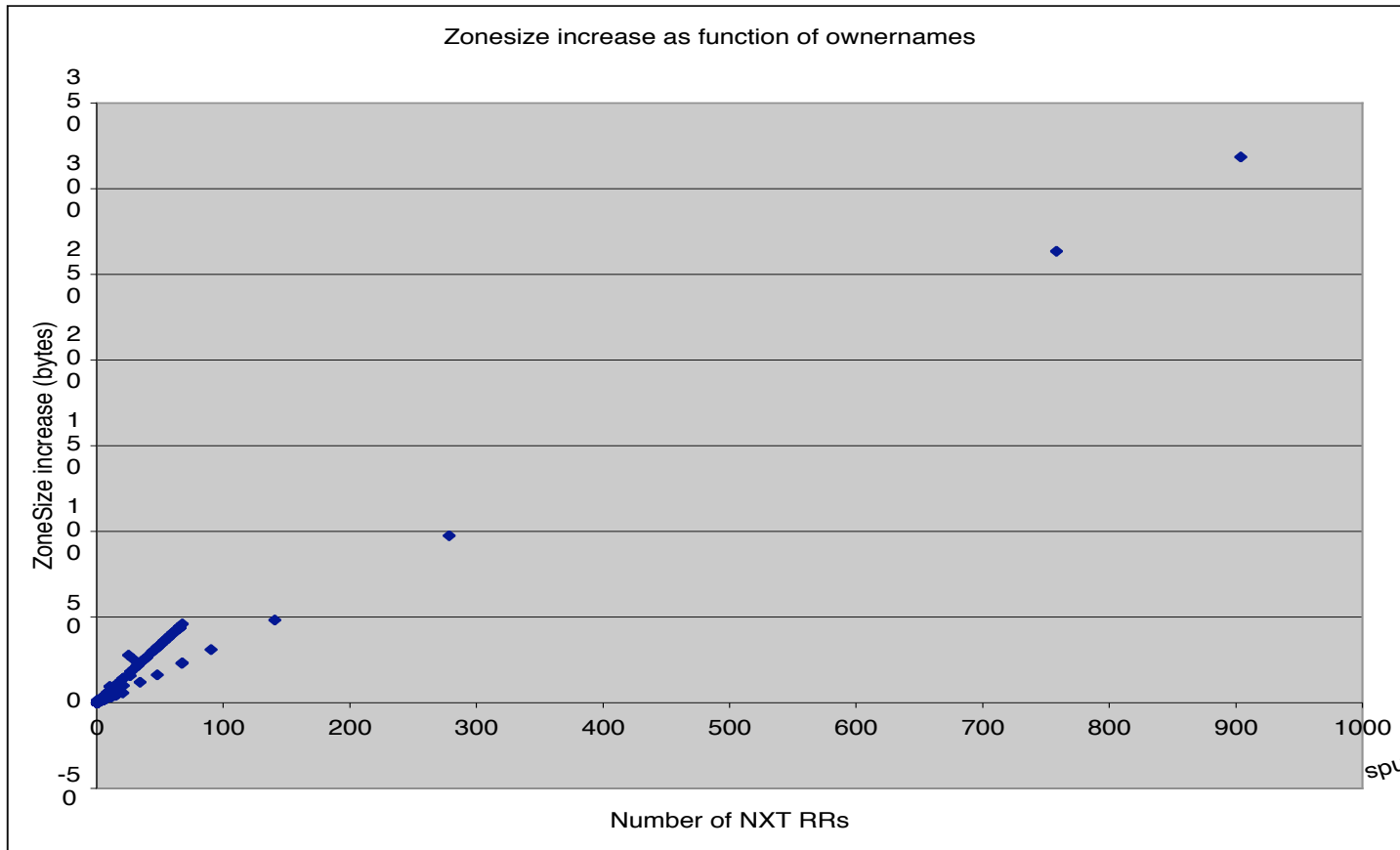


Some numbers

- A zone with mostly delegations
 - 1 NXT RR + SIG RR added
 - growth by about 350 bytes for every delegation.
- A “end-node”
 - 1 NXT+SIG and a SIG over PTR added
 - growth by about 672 bytes per owner name.
- Approximately 250/500 bytes per owner name in core respectivelye



Zone size increase per NXT (Size increase by signing)

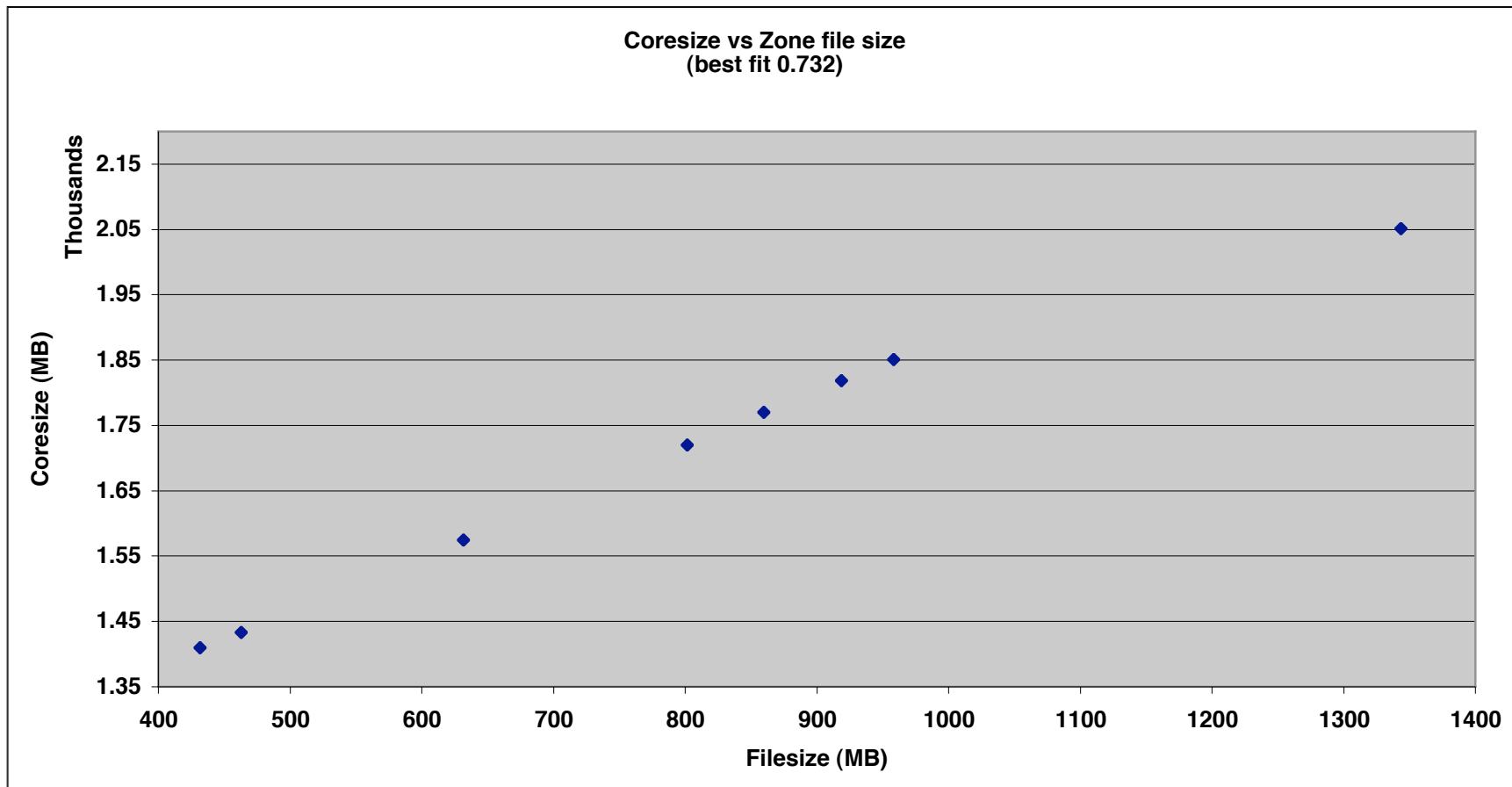


Bimodal distribution; 1 line best fitted by 350 byte/NXT
other

by 670 byte/NXT



NamedCore vs Filesize (size increase by signing)



Best fit: 0.72 Mb core increase/Mb file size increase



QUESTIONS?

- Slides available in the meeting archive:
www.ripe.net/....
- E-mail: disi@ripe.net