Yeti DNS: Status after a Year

Davey Song - 宋林健 / BII Labs / ljsong@biigroup.cn
Shane Kerr / BII Labs / shane@biigroup.cn

2016-07-17 / Berlin / IEPG
Previous Yeti Presentation in IEPG

Yeti DNS
IEPG July 2015

Shane Kerr / Bii Lab
2015-07-19 / Prague, Czech Republic
Goals of this presentation

1. Report Yeti status after one year
2. Ask for more traffic and more DNS guys to join us
Outline

- Yeti Project Motivation
- Project coordination & setup
- Yeti experiments and findings
- TODO & Lesson we learn
Related works and discussions on DNS Root system

- ICANN RSSAC Document (link)
- ICANN ITI Panel & technical report (link)
- ICANN Root Zone KSK Rollover (link)
- IETF document related to DNS Root system
  - RFC7626: DNS Privacy Considerations, by S. Bortzmeyer
  - RFC7706: Decreasing Access Time to Root Servers by Running One on Loopback, by W. Kumari, P. Hoffman
  - Initializing a DNS Resolver with Priming Queries (draft-ietf-dnsop-resolver-priming)
  - Experiences from Root Testbed in the Yeti DNS Project (draft-song-yeti-testbed-experience)
  - An IXFR Fallback to AXFR Case (draft-song-dnsop-ixfr-fallback)
- Scaling the Root by Geoff Huston, IPJ, March 2015 (link)
- Anycast vs. DDoS: Evaluating the November 2015 Root DNS Event, by Giovane, Ricardo etc. (link)
One slide for Yeti motivation

- Mainly Two concerns
  - External Dependency & Surveillance risk
  - New technologies or tries on Root system
- Yeti PS: https://github.com/BII-Lab/...doc/Yeti_PS.md
- Few studies on new model of DNS Root system, we want to have try and contribute a cent...
- Inspired by permissionless innovation

"a good design could allow a political process of deciding how control for a particular zone should be shared to start"

-- ICANN ITI technical report
One slide for Yeti status

- 3 DM using MZSK model to generate zone
- Current Yeti root servers & operators ([http://yeti-dns.org/operators.html](http://yeti-dns.org/operators.html))
  - 25 Yeti root servers (soon 26)
  - 14 Yeti root operators (soon 15)
- 400+ independent IP prefix visit us, 30+ regular resolvers, less than 100qps,
- 2 experiments done with some findings. Just kick off KSK rollover
- Currently response size up to 2134 Bytes
- 2016 Yeti Workshop in Seoul
  - Nov 12, one day before IETF
Technical Setup

- Machine
  - Most VPS
  - 3 physical machine

- OS system
  - more than half using Linux
  - Netbsd, FreeBSD
  - One server using Windows!

- DNS software
  - BIND9
  - NSD4.1.5, 4.1.0
  - Knot 2.0.1, 2.1.0
  - Windows DNS server,
  - PowerDNS
Technical Setup

- Web site, Mailman, Trac, Nagios, ...
- 3 distribution masters (DM)
  - Using shared git repository for synchronization
- Yeti participants (http://yeti-dns.org/operators.html)
  - 25 Yeti root servers (soon 26)
  - 14 Yeti root servers (soon 15)
- 30+ active resolvers
  - http://dsc.yeti-dns.org/dsc-grapher.pl?binsize...
Current Need: Traffic

- DNS caching is really efficient
- <100 queries/second
- Please help!
  - Set up a Yeti resolver
    [link](http://yeti-dns.org/join.html)
  - Use dnsdist with a Yeti resolver
    [link](http://yeti-dns.org/.../Mirroring-traffic-using-dnsdist.html)
  - Try the ymmv query mirror (alpha code)
    [link](https://github.com/shane-kerr/ymmv)
Experiments

- Yeti is for research!
- Experimental protocol
  - Lab test, List proposal, Experiment, Report
  - https://github.com/BII-Lab/.../Experiment-Protocol.md
- Queue of experiments
  - https://github.com/BII-Lab/.../Experiment-Schedule.md
Experiment: MZSK

- MZSK is "Multiple ZSK": separate ZSK for each DM
- Phase 1: lots of DNSKEY (1 KSK, 6 ZSK)
  - Simulates all ZSK rolling at once
- Phase 2: actual separate ZSK
- Various bugs: Linux kernel bug, IXFR issues, ...
- Completed, report written (pending data analysis)
- Future work:
  - Non-shared KSK
  - Zone verification by Yeti root servers
Experiment: BGZSK

- BGZSK is "Big ZSK": 2048 bit ZSK
- Moved to top of list by Verisign announcement
- Skipped lab test
- No surprises (good!)
- Completed, pending report
  - https://github/.../Experiment-BGZSK.md
Experiment: KROLL

- KROLL is "KSK roll": KSK roll
- Test root KSK roll before ICANN
- First of two experiments:
  - KROLL is normal double-DS KSK roll
  - IROLL is like the proposed ICANN roll
- Takes at least 30 days, maybe 60 days
- KROLL IN-PROGRESS
  - https://github.com/.../Experiment-KROLL.md
Pending Experiments

- RENUM: Root Server Renumbering
- 5011X: RFC 5011 Roll-Back
- FAKER: *Lots* of Root Servers
- DOT-Y: Rename Servers to .YETI-DNS
- PMTNC: Priming Truncation
- ECDSA: KSK ECDSA Roll
- FSTRL: Frequent ZSK Roll
- TCPRT: TCP-only Root

*New ideas are well come!*
TODO

• We are going to
  • Finish the Pending Experiments, deliver results and findings
  • Do fine grained research on yeti Data analysis
    • Try to use ENTRADA developed by SIDN http://entrada.sidnlabs.nl/
    • Present Yeti work to related bodies and Interested people
Lessons we learn so far

• It is always easier to say than to do
  • To build and operate a research testbed is systematic work
  • Yeti is started with inspiration but lack of full preparation
  • It is driven by Yeti community and people with questions, technical challenges, suspects… (still now)
• Coordination among Yeti participants are not a easy job!
  Current IANA Root operators deserve the credit
• More technical findings please refer to Yeti experience draft
Conclusion

• Results are finally appearing
• Don’t forget to send us queries!
• Join us at the next Yeti Workshop
  - Before IETF 97 in Seoul (2016-11-12)
  - Look for qualified speakers on Root server research
Image Credits

- Traffic:
  https://www.youtube.com/...0r004qlzJVQ

- Science:
  https://commons.wikimedia.org/...nd.svg