OARC 27th Workshop
San Jose, USA
30 September 2017

DNS-OARC Software

Jerry Lundström
Software Engineer

Software Projects & Funding

https://www.dns-oarc.net/oarc/software

- New overview page for software developed and maintained by OARC

- How to fund development, links to GitHub project pages and mailing lists

- OARC's Open-Source Software Licensing Policy

DNS-OARC
Domain Name System Operations Analysis and Research Center

DSC Releases

- v2.5.1
  - Various compatibility issues and a possible runtime bug, related to pcap-thread, fixed

- v2.6.0
  - New filters, configuration options and more compatibility issues fixed

- v2.6.1
  - Compatibility fixes for FreeBSD 11.1+ which is now packing struct ip

DNS-OARC
Domain Name System Operations Analysis and Research Center

DNSCAP Releases

- v1.4.1
  - Various compatibility issues and a possible runtime bug, related to pcap-thread, fixed

- v1.5.0
  - Support for gzip'ing PCAP output on-the-fly
  - New plugin rzkeychange
  - … and more compatibility issues fixed

- v1.5.1
  - Yes, you guessed it! Compatibility fixes!

DNS-OARC
Domain Name System Operations Analysis and Research Center

PacketQ Releases

- v1.3.0

  – First release under OARC management with license changed to GPL v3.0

  – Big endian, buffer overruns, s/sprintf/snprintf/, "time of check, time of use", automated regression tests and more

- v1.3.1

  – ICMP and EDNS parsing fixed

- v1.4.0

  – New fields for IP version and EDNS0 ECS

DNS-OARC
Domain Name System Operations Analysis and Research Center

DROOL Releases

- v1.0.0-beta.3

  – Various compatibility, pcap-thread and fuzzing fixes

- v1.0.0-beta.4

  – Compatibility fixes and packaging

- v1.0.0-rc.1

  – Usage documentation and man-pages

  – Best effort timing mode

  – Correct nanosleep() usage

DNS-OARC
Domain Name System Operations Analysis and Research Center

Packages

https://dev.dns-oarc.net/packages

- Debian: Jessie, Stretch, **Buster**, Sid

- Ubuntu: Trusty, Xenial, Zesty, **Artful**

- **EPEL**: 6, 7

- **Fedora**: 25, 26, 27, rawhide

- **SLE**: 12, 12 SP1, 12 SP2

- **OpenSUSE**: 42.2, 42.3, Tumbleweed

- FreeBSD, OpenBSD: Links to ports packages

DNS-OARC
Domain Name System Operations Analysis and Research Center

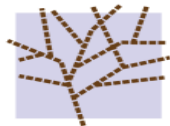# Check My DNS v2

https://cmdns.dev.dns-oarc.net

- Rewritten in Go

- New GUI using WebSocket for speedy interaction

- Using real DNS authority server software as backends

- Testing normal DNS, TCP, IPv6, DNSSEC, QNAME minimisation and **DNS ID + port number randomization**

DNS-OARC
Domain Name System Operations Analysis and Research Center

New Projects

Root Server Statistic Measurements

- Project funded by Verisign
- Update the RSSM plugin for DNSCAP to RSSAC002v3
  - Output RSSAC002v3 YAML
  - Scripts for merging RSSAC002v3 YAML results
- Improve capturing
  - Reassemble IP v4/v6 fragments
  - Support ongoing TCP session

DNS-OARC
Domain Name System Operations Analysis and Research Center

"Bad" Packets

https://github.com/DNS-OARC/bad-packets

- Repository of PCAPs and scripts to generate packets that can be used for testing software

- Using scapy to generate IP v4/v6 fragments

  – Missing fragments, one off, empty, duplicated, wrong flags, reordered and fuzzed

- More additions are welcomed!

DNS-OARC
Domain Name System Operations Analysis and Research Center

DROOL

- Continued development funded by Comcast Innovation Fund

  – Parse and match responses from the packets being replayed

  – Better thread performance

  – More statistical output

- Work targeted for 2018

DNS-OARC
Domain Name System Operations Analysis and Research Center

Questions?

(if we have time)

DNS-OARC
Domain Name System Operations Analysis and Research Center