OARC 29th Workshop
Amsterdam, NL
13 October 2018

DNS-OARC Software

Jerry Lundström
Software Engineer
jerry@dns-oarc.net

Software Projects & Funding

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

- Overview of software developed and maintained by OARC
  - dnsjit – Engine for capturing, parsing and replaying DNS
  - drool – DNS Replay Tool
  - dsc – DNS Statistics Collector with legacy presenter or Grafana
  - dnscap – Network capture utility designed specifically for DNS traffic
  - packetq – Use SQL on PCAPs
- Information about funding development, licensing policy, links to GitHub project pages and mailing lists

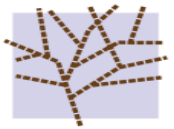
dnsjit

https://github.com/DNS-OARC/dnsjit

“dnsjit is a combination of parts taken from dsc, dnscap, drool, and put together around Lua to create a script-based engine for easy capturing, parsing and statistics gathering of DNS message while also providing facilities for replaying DNS traffic.”

dnsjit

- v0.9.6 alpha packages available
- Changes since OARC 28:
  - No more submodules
  - Overall performance improvements
  - New core objects representing network stack and payloads
  - New producer interface to get objects
  - New thread and channel facility



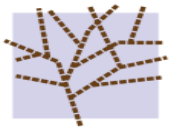
DNS-OARC
Domain Name System Operations Analysis and Research Center

drool

- v1.99.3 alpha packages available
- Now written in Lua using dnsjit
- Configs replaced with command

```
$ drool <command> [options]
```

- Commands for each scenario
- Funded by Comcast



DNS-OARC
Domain Name System Operations Analysis and Research Center

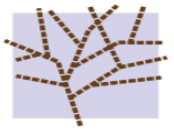
drool replay

- Replay DNS traffic from packet capture (PCAP)
  - Match timing and protocol as recorded
  - Replay as UDP or TCP
  - Manipulate timing between packets to speed up or slow down
  - Skip timing and just blast away

drool replay example

- Send all DNS queries twice as fast as found in the PCAP file to localhost using UDP

```
$ drool replay \
  --timing multiply=0.5 \
  --no-tcp \
  file.pcap 127.0.0.1 53
```

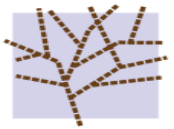


DNS-OARC
Domain Name System Operations Analysis and Research Center

drool replay example

- Send all DNS queries over TCP to localhost as they were recorded

```
$ drool replay \
  --timing keep \
  --no-udp \
  file.pcap 127.0.0.1 53
```

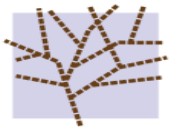


DNS-OARC
Domain Name System Operations Analysis and Research Center

drool replay example

- Take all DNS queries found in the PCAP file and send them as fast as possible over UDP to localhost by ignoring both timings, replies and starting 3 threads that will simultaneously send queries.

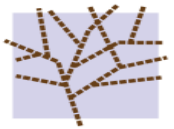
```
$ drool replay \
  --no-tcp --no-responses \
  --threads --udp-threads 3 \
  file.pcap 127.0.0.1 53
```



DNS-OARC
Domain Name System Operations Analysis and Research Center

drool respdiff

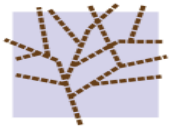
- Replay DNS traffic, if both query and response is found, from packet capture (PCAP) and store results in a Lightning Memory-Mapped Database (LMDB)
  - Result can be analyzed with respdiff, tool-chain from Knot project by CZ.NIC
  - Compare responses in PCAP with received responses
  - Configure respdiff to compare different parts of the responses



drool respdiff example

- Replays a PCAP file against localhost and then uses the respdiff tool-chain to analyze the results

```
$ drool respdiff /lmdb/path \
  pcap file.pcap \
  target 127.0.0.1 53
$ msgdiff.py /lmdb/path
$ diffsum.py /lmdb/path
```

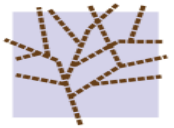


DNS-OARC
Domain Name System Operations Analysis and Research Center

respdiff output example

```
== Global statistics
duration                          2            seconds
queries                          41
answers                          41  100.00 % of queries

== Differences statistics
upstream unstable                 0    0.00 % of answers (ignoring)
not 100% reproducible             0    0.00 % of answers (ignoring)
target disagrees                  0    0.00 % of not ignored answers
```



DNS-OARC
Domain Name System Operations Analysis and Research Center

dsc

- v2.7.0
  - Additional link layer support (LINUX_SLL)

dsc

https://dsc-dnstap.dev.dns-oarc.net

- Preliminary DNSTAP input support, **try it!**
  - Unbound → DSC+DNSTAP → dsc-datatool → Grafana
  - Resolver open for RIPE and Okura network during OARC29
    - 2a01:3f0:0:57::249
    - 77.72.225.249

```
$ dig @dsc-dnstap.dev.dns-oarc.net <...>
```

dsc

- Response Time Statistics
  - Funded by NIC.AT
  - Counter per response time bucket (configurable), 0-10ms 10-20ms etc
  - Counter on only query, only response and removed query/response from tracking due to memory limitations and timeouts
  - Aiming for release in late January 2019

dnscap

- Upcoming version will get built in anonymization capability
  - Funded by Verisign
  - Using methods proposed in RSSAC040 “Recommendations on Anonymization Processes for Source IP Addresses Submitted for Future Analysis”
  - Aimed to be released 2018Q4

Continuous Integration

- Replaced Jenkins with Buildbot
  - Jenkins and OpenBSD did not play well together
  - Quite nice to remove dependency on Java
- Platform update
  - Reinstall all platforms with latest stable
  - Ubuntu 18.04, Debian 9.5, CentOS 7.5, FreeBSD 11.2 and OpenBSD 6.3

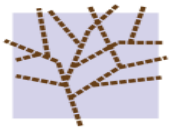
OARC Portal v2

- Reworked from the ground up!
  - Using python flask and bootstrap
- First release will keep existing functionality except...
  - Password reset without PGP
  - Look and feel is quite different
- Future releases will integrate more!
  - Sign-up of new members and management of access to services

Questions...

Come by the Demo Booth!

- Showcasing OARC's software, tools and services
- Hands-on with dnsjit, drool, dnscap and packetq
- Click around in new Portal v2, DSC+DNSTAP Grafana and Check My DNS
- Code your own Lua/dnsjit program!



DNS-OARC
Domain Name System Operations Analysis and Research Center