DNSharness:
A Tool for DNS Researchers

Paul Hoffman

Tech Day, ICANN 50

June, 2014

v1

DNSharness in one slide

- A test harness for automated sending queries to numerous DNS authoritative and recursive servers
- Comes with lots of open source software prebuilt
- Aimed at DNS researchers, developers, and anyone who wants to iteratively test DNS against a variety of servers
- Can be used for many types of tests such as DNSSEC, new RRtypes, and so on
- Allows publishing of tests so that others can reproduce and tweak

DNSharness basics

- Python script running on a Linux box that also has VirtualBox for VMs
- All open source DNS lives on one VM, each built into its own directory
- You add projects, each of which lives in its own directory
- You can also test on systems running outside the Linux box, such as DNS hardware and open recursive resolvers

Open source servers included

- All buildable versions of many servers
- BIND 8, 9, and 10
- DNSMASQ
- Knot
- NSD
- PowerDNS
- Unbound

What a project directory looks like

- Project description file (short JSON object)
- Program that runs on the Linux host at start up, for each test step, and on shutdown
- Program that sets up and tears down the software running on the VM with the open source, and associated config files

Project description file, example #1

```
{
  "name" : "Authoritative with CD",
  "comment1" : "Some comment goes here",
  "targets" : [
     { "opensource" : [ "bind-9.6.*”,
                  "bind-8.4.*", "nsd.*" ] }
  ]
}
```

Project description file, example #2

```
{
  "name" : ”Recurse with broken request",
  "targets" : [
   { "winserv2003" : [ "10.20.30.203" ] },
   { "winserv2008" : [ "10.20.30.208" ] },
   { "GoogleDNS" : [ "8.8.8.8", "8.8.4.4" ] }
  ]
}
```

Program that runs on the Linux host

- Actions for start up and shutdown
- Run each time a project step starts and stops
  - For example, start up a VM, alert the tester for a certain test, ...
- Runs in the middle of each step to send the request to the server being tested
  - Query can be `dig`, a `getdns`-based program, or from the new ZoneBuilder

Program that runs on VM with open source software

- Starts up the particular DNS server with the right config files and initialization commands
- Can be complex: DNSSEC sign a zone, do a quick key rollover, then respond to queries
- Tears it down, maybe saving any interesting log information

Speed

- In many applications, it takes less than 1 second per server to start it up, send the query, get the response, and shut it down cleanly
  - All 268 authoritative servers in the harness: 148 seconds on a slow laptop
- Recursion out to the Internet of course takes more time, but is still tractable for experiments
  - All 306 recursive servers going out for answers: 383 seconds

Includes a zone builder for sending odd queries and responses

- Easy to create zones with subtly or terribly broken responses to see how clients react
- Easy to create legal but weird queries (a query with multiple Question sections, a query that has an Answer section, ...)
- Can also be used for fuzzing

Includes `getdns` API

- Queries can come from `dig`, but can also come from `getdns`
- The `getdns` library is excellent for DNSSEC testing because you can easily dump all of the DNSSEC records that come back in a reply
- Also good for analyzing full responses

DNSharness project status

- First release in late 2012
- Full source and instructions at www.dnsharness.org
- Development was funded by VeriSign Labs (thank you!)
- For more information, contact me at paul.hoffman@vpnc.org
- Contact me this week if you want to see some demos