DNSSEC for legacy applications

libnss_getdns, a getdns nsswitch module as an alternative for the system stub

Willem Toorop
19 November 2015
DNS-WG @ RIPE71
Genesis

getdns API is

- A DNS API specification
  by and for application developers
  (for resolving)
  (for application)

- First implementation by VERISIGN Labs and NLnet Labs

From Verisign:
  Theogene Bucuti, Craig Despeaux,
  Angelique Finan, Neel Goyal,
  Scott Hollenbeck, Shumon Huque,
  Sanjay Mahurpawar, Allison Mankin,
  Sai Mogali, Prithvi Ranganath,
  Rushi Shah, Vinay Soni, Bob Steagall,
  Gowri Visweswaran, Glen Wiley

From NLnet Labs:
  Olaf Kolkman, Benno Overeinder,
  Willem Toorop, Wouter Wijngaards

From Sinodun:
  Sara and John Dickinson

From No Mountain Software:
  Melinda Shore
Genesis

• Give *applications* a better handle on DNS, ie:
  – Asynchronous
  – Get resource records other then A and AAAA
  – Get DNSSEC status for DANE
Genesis

- Give *applications* a better handle on DNS, ie:
  - Asynchronous
  - Get resource records other then A and AAAA
  - Get DNSSEC status for DANE, *but also signalling!*
Genesis

• Give *applications* a better handle on DNS, ie:
  – Asynchronous
  – Get resource records other then A and AAAA
  – Get DNSSEC status for DANE, *but also signalling!*

• Many *features* don't need *application interface*
  – TCP Pipelining, Keep connections open, TCP Fast Open
  – DNS over TLS
Many features don't need application interface
- TCP Pipelining, Keep connections open, TCP Fast Open
- DNS over TLS
- DNSSEC iteration as STUB
Give applications a better handle on DNS, ie:
– Get resource records other than A and AAAA
– Asynchronous
– Get DNSSEC status for DANE

Many features don’t need application interface:
– TCP Pipelining, Keep connections open, TCP Fast Open
– DNS over TLS
– DNSSEC iteration as STUB
– Since version 0.5.1, Roadblock Avoidance
- From Xavier's presentation:
  - 64% provide DNSSEC for existing things
  - 56% provide DNSSEC proof for Denial of Existence
  - 40% provide DNSSEC for wildcards

- Since version 0.5.1, Roadblock Avoidance
• From Xavier's presentation:
  • 64% provide DNSSEC for existing things
  • 56% provide DNSSEC proof for Denial of Existance
  • 40% provide DNSSEC for wildcards
• draft-ietf-dnsop-dnssec-roadblock-avoidance
• Minimal passive implementation: *on BOGUS, retry with full recursion*

– Since version 0.5.1, Roadblock Avoidance
• From Xavier's presentation:
  • 64% provide DNSSEC for existing things
  • 56% provide DNSSEC proof for Denial of Existance
  • 40% provide DNSSEC for wildcards
• draft-ietf-dnsop-dnssec-roadblock-avoidance
• Minimal passive implementation: on BOGUS, retry with full recursion

– Since version 0.5.1, Roadblock Avoidance
- Configure enterprise perimeter network devices to block all outbound User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) traffic to destination port 53, except from specific, authorized DNS servers (including both authoritative and caching/forwarding name servers).

- Minimal passive implementation: on BOGUS, retry with full recursion

- Since version 0.5.1, Roadblock Avoidance

https://www.us-cert.gov/ncas/alerts/TA15-240A
Genesis

- Many *features* don't need *application interface*

- Linux and Unix systems provide a default DNS resolver library
  - Applications perform name resolution via `getaddrinfo()`, `getnameinfo()`, etc.

- Current library implementations do not support DNSSEC nor other modern DNS capabilities
Enhanced system wide lookup using getdtns

A summer student project

executed at VERISIGN LABS, by

Theogene H. Bucuti, University of North Texas

Supervised by: Gowri Visweswaran and Allison Mankin

Explore the ways to provide an alternative for the system's stub resolver, adding modern DNS capabilities such as security and privacy, and compare the usability, possibilities and impossibilities of the different options.
Enhanced system wide lookup using getdns

- **libnss_getdns**
  - *Open Source* module that provides DNSSEC validation for legacy systems through the Linux/Unix name resolution framework (*nsswitch*) using the getdns library

- [https://github.com/getdnsapi/libnss_getdns](https://github.com/getdnsapi/libnss_getdns)
- Works for: Firefox, Opera, Links2, Epiphany, lynx, curl, wget, ssh, ping, telnet, etc.
- Does not work for Google Chrome & Chromium
- Also **LD_PRELOAD** based version. *Not recommended*
libnss_getdns

Configuration

- In `/etc/nsswitch.conf` replace `dns` with `getdns`
libnss_getdns

Configuration

• In `/etc/nsswitch.conf` replace `dns` with `getdns`

```conf
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
hosts:       files mdns4_minimal [NOTFOUND=return] getdns mdns4
networks:   files
```

• **Issue:** Many of the modern DNS capabilities have `state`:
  – State full transports (TCP & TLS)
  – The cache with full recursion
  – Upstream capability tagging etc.
  all contained in a `getdns_context`
libnss_getdns
Configuration

- In /etc/nsswitch.conf replace dns with getdns

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.

hosts:          files mdns4_minimal [NOTFOUND=return] getdns mdns4
networks:      files
```

- **Issue**: Many of the modern DNS capabilities have state all contained in a getdns_context
- `$ ./getdns_daemon`
libnss_getdns
Configuration

- In `/etc/nsswitch.conf` replace `dns` with `getdns`

```bash
# /etc/nsswitch.conf
# Example configuration of GNU Name Service Switch functionality.
hosts:    files mdns4_minimal [NOTFOUND=return] getdns mdns4
networks: files
```

- **Issue**: Many of the modern DNS capabilities have `state` all contained in a `getdns_context`
- `$ ./getdns_daemon`
- `configure --disable-daemon-only-mode`
- `configure --without-context-proxy`
- `configure --with-context-proxy=dbus`

*Not recommended*
libnss_getdnd

Configuration

- User level config:
  ~/.getdns/preferences.conf

- Global level config:
  /etc/getdns.conf

# /etc/getdns.conf
dnssec: roadblock_avoidance
tls: prefer_tls
logging: critical

Browsers will need to be restarted for changes to apply.
libnss_getdns
In path signalling
libnss_getdns

In path signalling

- Better approach: Desktop notifications
- Offer to add negative trust anchor
Summary

- **DNSSEC-capable** alternative to the system’s stub resolver
- ** Seamlessly** enforce **secure** and **private** name resolution
- Avoid **DNSSEC roadblocks**
- **Customisable** at system and user level
- **DNSSEC failure signalling** (http only)

**Warning!**
An exploring study. Code is a collection of many different try outs. Use for experimentation only. Do not use in production!

roadblock_avoidance extension needs much more work too

**github repo** https://github.com/getdnsapi/libnss_getdns
**me** Willem Toorop <willem@nlnetlabs.nl>