getdns API implementation

Willem Toorop

Willem@NLnetLabs.nl

NLnet Labs

14 May 2014

getdns Unbound security API is:

- A *DNS API* specification (for resolving)
  by and for application developers (for applications)
- First implementation by VERISIGN LABS and NLnet Labs

From Verisign:

Allison Mankin, Glen Wiley, Neel Goyal, Angelique Finan, Craig Despeaux, Shumon Huque, Duane Wessels, Gowri Visweswaran

From NLnet Labs:

Willem Toorop, Wouter Wijngaards, Olaf Kolkman

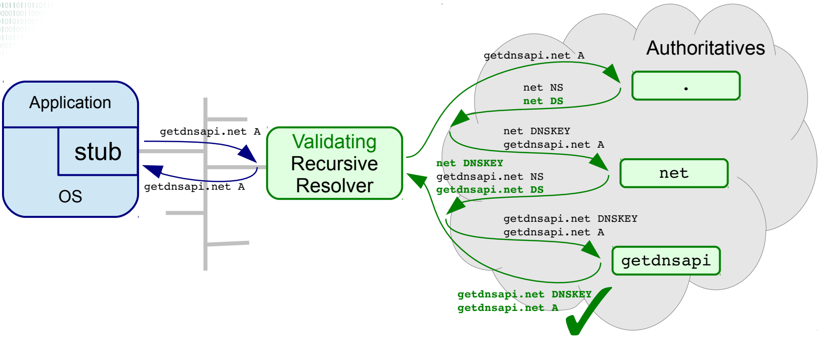
From No Mountain Software:

Melinda Shore

From Sinodun:

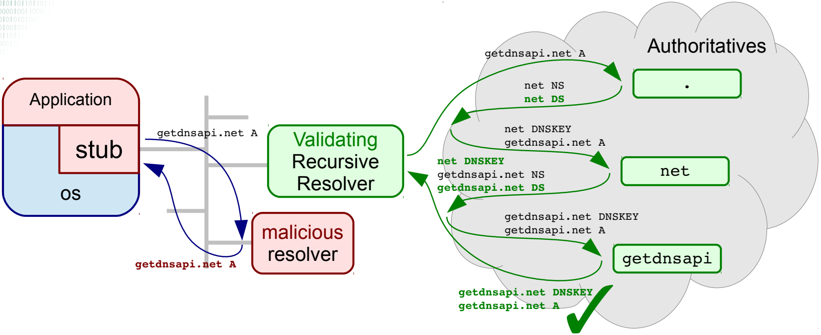
John & Sara Dickinson

Motivation - DNSSEC - The Last Mile



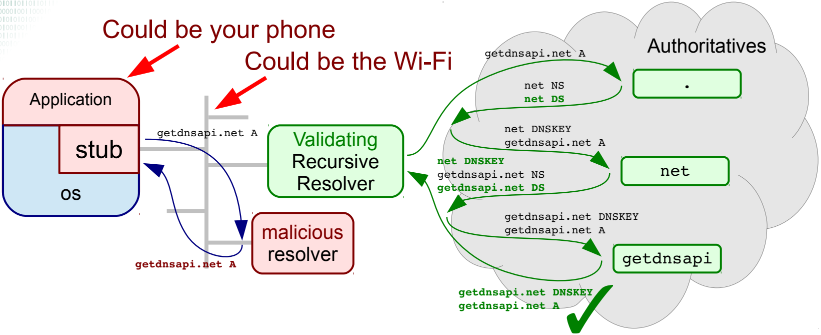
- A DNSSEC enabled resolver protects against cache poisoning
- Application does not know an answer is secure (AD bit not given with `getaddrinfo()`)

Motivation - DNSSEC - The Last Mile



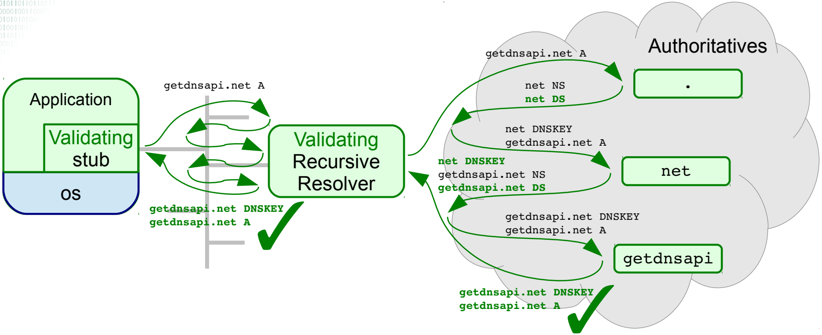
- A DNSSEC enabled resolver protects against cache poisoning
- Application does not know an answer is secure
- Is the local network resolver trustworthy?

Motivation - DNSSEC - The Last Mile



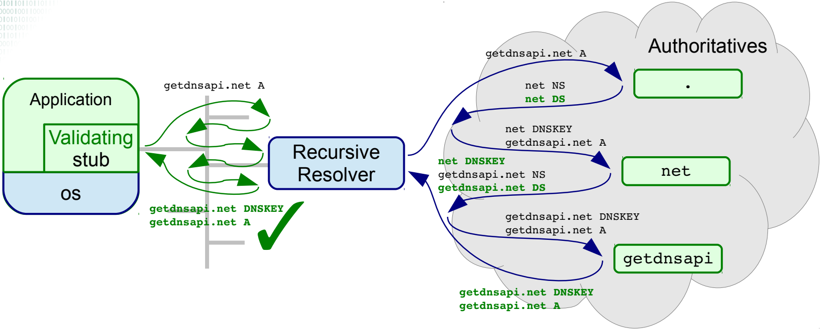
- A DNSSEC enabled resolver protects against cache poisoning
- Application does not know an answer is secure
- Is the local network resolver trustworthy?

Motivation - DNSSEC - The Last Mile



- A DNSSEC enabled resolver protects against cache poisoning
- Application does not know an answer is secure
- Is the local network resolver trustworthy?

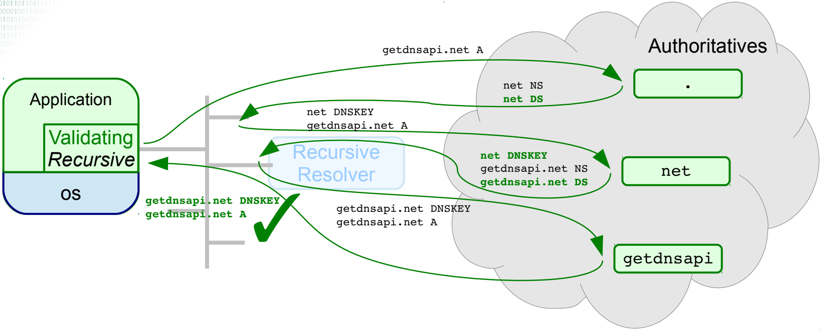
Motivation - DNSSEC - The Last Mile



- A DNSSEC enabled resolver protects against cache poisoning
- Application does not know an answer is secure
- Is the local network resolver trustworthy?
- Is the local network resolver validating?

  (90% of RIPE ATLAS probes have a DNSSEC-aware resolver
  Presentation later this morning right here at the DNS-WG session)

Motivation - DNSSEC - The Last Mile



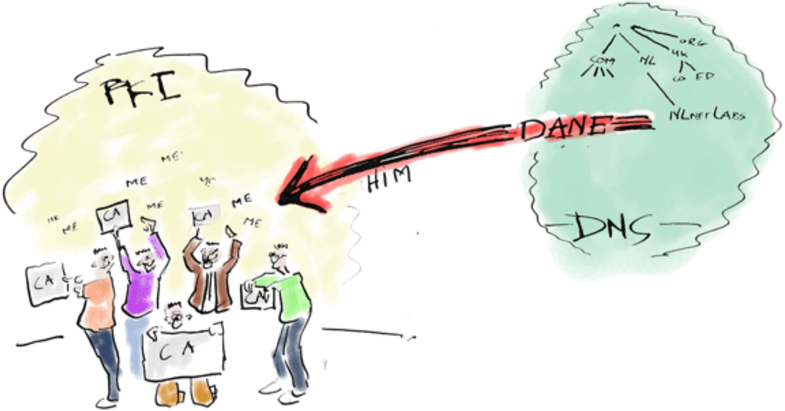
- A DNSSEC enabled resolver protects against cache poisoning
- Application does not know an answer is secure
- Is the local network resolver trustworthy?
- Is the local network resolver validating?
- And when it is not even DNSSEC-aware?

Motivation - DNSSEC - DANE

- A DNSSEC enabled resolver protects against cache poisoning
- By giving authenticated answers (origin authentication)
- Enabling **D**NS-based **A**uthentication of **N**amed **E**ntities

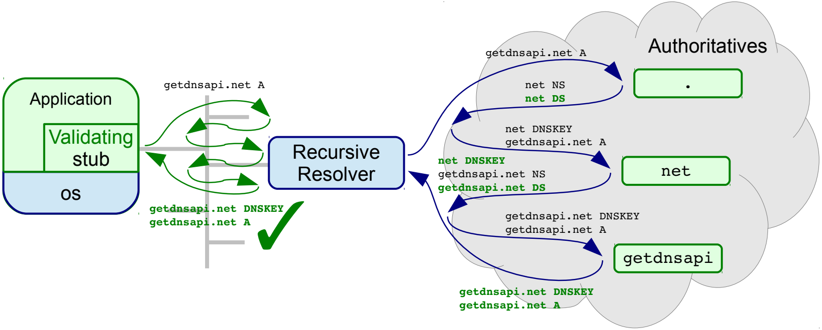
Motivation - DNSSEC - DANE

- Enabling **D**NS-based **A**uthentication of **N**amed **E**ntities
- For example to authenticate a TLS certificate
- Trust only self chosen TLD (+ the root)
  instead of ... 50? ... 500? ... more?



Motivation - DNSSEC - DANE

- Enabling **D**NS-based **A**uthentication of **N**amed **E**ntities
- For example to authenticate a TLS certificate
- Trust only self chosen TLD (+ the root) instead of ... 50? ... 500? ... more?



- A global distributed database of authenticated data

Implementation - Features

- Both stub and full recursive modes (recusive by default)
- Asynchronous modus operandi is the default
- Modular event base: libevent, libev, libuv, file descriptor
- Delivers validated DNSSEC in every way (off by default :( )
- JSON like response dict type
- javascript (node) and python language bindings

Implementation - Supported platforms

We support

- Debian 7.0, 7.3
- FreeBSD 8.4, 9.2, 10.0
- RHEL/CentOS 6.4, 6.5
- OSX 10.8, 10.9
- Ubuntu 12.04, 13.10

We provide binary packages for

- CentOS/RHEL 6.5
- MacOS X

Packages are available for

FreeBSD Via ports

MacOS X Via homebrew

Packages in the make

Debian Ondřej Surý

Fedora Paul Wouters

MS-Windows and Android in the future

Implementation - Building / Dependencies

- Get the tarball:
  `http://getdnsapi.net/dist/getdns-0.1.1.tar.gz`
- or `git clone http://github.com/getdnsapi/getdns`

libunbound For resolving

(Currently both recursive and stub)

libldns For parsing and constructing wire-format DNS data

(Will do the stub resolving in future releases)

libidn1 For `getdns_convert_ulabel_to_alabel()`
and `getdns_convert_alabel_to_ulabel()`

Pluggable event library extensions

One or more of: libevent 1, libevent 2, libuv, libev

- Build dependency: doxygen
- Install dependency: unbound-anchor

The Next Web - Hack Battle - 23 & 24 April 2014 A'dam

The Next Web - Hack Battle - 23 & 24 April 2014 A'dam

verify'EM

- Arvind Narayanan, Bhavna Soman & Ruslan Mavlyutov
- Plugin for Thunderbird gives information on the DNSSEC credentials of DKIM records associated with e-mail

DANE Doctor

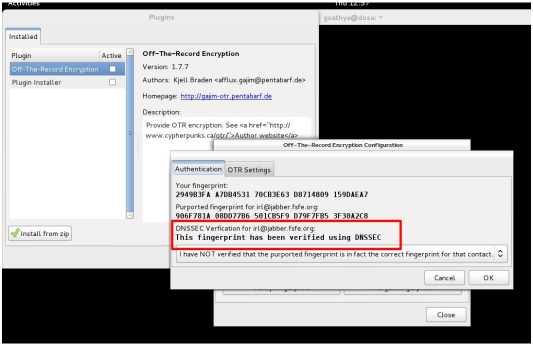
- Hynek Schlawack and Richard Wall
- Diagnostics webapp for DANE
- DANE enabled TLS client API to the asynchronous event framework Twisted.
- `https://github.com/hynek/tnw`

The Next Web - Hack Battle - 23 & 24 April 2014 A'dam

Bootstrapping Trust with DANE

- Sathya Gunasekaran and Iain Learmonth.
- Adds DNSSEC secured OTR-key lookups to Gajim XMPP client

- `https://github.com/irl/dnskeys`
- `https://github.com/gsathya/gotr`



Off-The-Record Encryption

Version: 1.7.7

Authors: Kjell Braden <afflux.gajim@pentabarf.de>

Homepage: http://gajim-otr.pentabarf.de

Description:

Provide OTR encryption. See <a href="http://www.cypherpunks.ca/otr/">Author website</a>

Your fingerprint:
`2949B3FA A7DB4531 70CB3E63 D8714809 159DAEA7`

Purported fingerprint for irl@jabber.fsfe.org:
`906F781A 08DD77B6 501CB5F9 D79F7FB5 3F30A2C8`

DNSSEC Verfication for irl@jabber.fsfe.org:
`This fingerprint has been verified using DNSSEC`

I have NOT verified that the purported fingerprint is in fact the correct fingerprint for that contact.

- interview @ tweakers.net
- slides deck

The Next Web - Hack Battle - 23 & 24 April 2014 A'dam

DNSSEC name and shame

- ✘ sendgrid.com
- ✘ deezer.com
- ✔ labs.verisigninc.com
- ✘ www.spotify.com
- ✔ blueprint.paypal.com
- ✘ www.pearson.com
- ✘ twitter.com
- ✘ mashery.com
- ✘ push.co

- Joel Purra & Tom Cuddy
- Shame the non DNSSEC APIs
- `http://dnssec-name-and-shame.com/`
- `https://github.com/joelpurra/node-dnssec-name-shame`

Security starts with a name

getdns
Unbound security

website	http://getdnsapi.net
github repo	http://github.com/getdnsapi/getdns
python repo	http://github.com/getdnsapi/getdns-python-bindings
node repo	http://github.com/getdnsapi/getdns-node
mailing-list	http://getdnsapi.net/mailman/listinfo/users
TNW Hackathon	https://www.hackerleague.org/hackathons/kings-of-code-hack-battl
TNW Videos	https://www.youtube.com/channel/UCF0NmkWgpS0KDHJqrWw8-5w
API website	http://www.vpnc.org/getdns-api
API list	http://www.vpnc.org/mailman/listinfo/getdns-api
me	Willem Toorop <willem@nlnetlabs.nl>