DNSSEC

From **W:Domain Name System Security Extensions**:

> The Domain Name System Security Extensions (DNSSEC) is a suite of Internet Engineering Task Force (IETF) specifications for securing certain kinds of information provided by the Domain Name System (DNS) as used on Internet Protocol (IP) networks. It is a set of extensions to DNS which provide to DNS clients (resolvers) origin authentication of DNS data, authenticated denial of existence, and data integrity, but not availability or confidentiality.

Related articles

Unbound#DNSSEC validation

Contents

Basic DNSSEC validation

Note: Further setup is required for your DNS lookups DNSSEC by default. See **#Install a DNSSEC-aware validating recursive server** and **#Enable DNSSEC in specific software**.

Installation

The *drill* tool can be used for basic DNSSEC validation. To use *drill*, **install** the **`ldns (https://www.archlinux.org/packages/?name=ldns)`** package.

Query with DNSSEC validation

Then to query with DNSSEC validation, use the `-D` flag:

```
$ drill -D example.com
```

Testing

As a test use the following domains, adding the `-T` flag, which traces from the rootservers down to the domain being resolved:

```
$ drill -DT sigfail.verteiltesysteme.net
```

The result should end with the following lines, indicating that the DNSSEC signature is bogus:

```
[B] sigfail.verteiltesysteme.net.       60      IN      A       134.91.78.139
;; Error: Bogus DNSSEC signature
;;[S] self sig OK; [B] bogus; [T] trusted
```

Now to test a trusted signature:

```
$ drill -DT sigok.verteiltesysteme.net
```

The result should end with the following lines, indicating the signature is trusted:

```
[T] sigok.verteiltesysteme.net. 60      IN      A       134.91.78.139
;;[S] self sig OK; [B] bogus; [T] trusted
```

Install a DNSSEC-aware validating recursive server

To use DNSSEC system-wide, you can use a validating recursive resolver that is DNSSEC-aware, so that all DNS lookups go through the recursive resolver. **BIND** and **unbound** are two options that you can setup. Note that each requires specific options to enable their DNSSEC validation feature.

If you attempt to visit a site with a bogus (spoofed) IP address, the valiging resolver (i.e., BIND or unbound) will prevent you from receiving the invalid DNS data and your browser (or other application) will be told there is no such host. Since all DNS lookups go through the valiging resolver, you do not need software that has DNSSEC support built-in when using this option.

Enable DNSSEC in specific software

If not you choose not to **#Install a DNSSEC-aware validating recursive server**, you need to use software that has DNSSEC support builtin in order to use its features. Often this means you must patch the software yourself. A list of several patched applications is found **here (https://www.dnssec-tools.org/wiki/index.php?title=DNSSEC_Applications)**. Additionally some web browsers have extensions or add-ons that can be installed to implement DNSSEC without patching the program.

DNSSEC Hardware

You can check if your router, modem, AP, etc. supports DNSSEC (many different features) using **dnssec-tester (http://www.dnssec-tester.cz/)** (Python and GTK+ based app) to know if it is DNSSEC-compatible, and using this tool you can also upload gathered data to a server, so other users and manufacturers can be informed about compatibility of their devices and eventualy fix the firmware (they will be probably urged to do so). (Before running dnssec-tester please make sure, that you do not have any other nameservers in `/etc/resolv.conf`). You can also find the results of performed tests on the **dnssec-tester (http://www.dnssec-tester.cz/)** website.

See also

- **DNSSEC Resolver Test (http://dnssec.vs.uni-due.de/)** - a simple test to see if you have DNSSEC implemented on your machine.
- **DNSSEC-Tools (https://www.dnssec-tools.org/)**
- **DNSSEC Visualizer (http://dnsviz.net)** - a tool for visualizing the status of a DNS zone.
- **RedHat: Securing DNS Traffic with DNSSEC (https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Security_Guide/sec-Securing_DNS_Traffic_with_DNSSEC.html)** - thorough article on implementing DNSSEC with *unbound*. Note that some tools are RedHat specific and not found in Arch Linux.
- **Wikipedia:Domain Name System Security Extensions**