BIND and root key rollover

Mukund Sivaraman

muks@isc.org

Internet Systems Consortium

Default trust anchors in BIND

- In BIND, the **bind.keys** file contains initial/starting trust anchors for the resolver for the **root zone**.
- When **dnssec-validation** is set to **yes**, no default trust anchor is used automatically. When **dnssec-validation** is set to **auto**, the keys in **bind.keys** file are used (for root only).
- For simpler configuration, a non-changeable copy of the default trust anchors is also built into the **named** program binary. If a **bind.keys** file exists, that will have precedence over the built-in copy.
- Non-root trust anchors need to be explicitly configured.

Manual trust anchor maintenance

- The **trusted-keys** config option is used to introduce manually maintained trust anchors to **named**. Such trust anchors are not automatically updated.
- Without RFC 5011 feature, when the root key changes the root trust anchors would have to be updated manually, otherwise DNSSEC validation would fail.
- **bind.keys** (root zone) configures itself for RFC 5011 automatic trust anchor maintenance (**managed-keys**).

Automatic trust anchor maintenance

- RFC 5011 feature in BIND is known as **managed-keys** after the **named** config option. It was introduced in BIND 9.7.0.
- **bind.keys** provides initial/starting trust anchor configuration as **managed-keys** that have not been rolled. It is an input file that is **not modified** by **named**.
- **named** creates a corresponding **managed-keys.bind** or **viewname.mkeys** database file which contains keys in various states, including current trust anchors.
- After a root key rollover, the keys in **bind.keys** may become stale and invalid whereas the managed keys database is used for trust anchors.

Quirks

- **named** uses master files to store the managed key database.
- Private RRTYPE code of 65533 is used to hold the key material and metadata.
- For new views, initial trust anchors will be taken from **bind.keys**, so a current copy should be provided by the admin.

Recommendations

- Visit Warren Kumari's website **http://keyroll.systems/** for resources on testing key rollover.
- Update the **bind.keys** file to the latest copy (when updates are released) as it provides the initial/starting root trust anchors for BIND builds that pre-date any root key rollovers.
- We publish the **bind.keys** file at **https://www.isc.org/bind-keys** and it will be updated when additional (future) root keys are available for distribution. The file also ships as part of the BIND source code and new releases will automatically have the latest copy of the file.