BIND 9.7
DNSSEC for Humans

Peter Losher
OARC
Beijing, November 2009

Agenda

- BIND and DNSSEC
- Why Do I Want DNSSEC?
- Why DNSSEC for Humans?
- BIND 9.7 Features
- How to get BIND 9.7

Why do I want DNSSEC?

- DNSSEC has come of age
- The root zone will be signed within the next year
- It's the right thing to do…

Why DNSSEC for Humans?

An example of why we call this release "DNSSEC for Humans"

Take the previous commands for creating a typical set of DNSSEC keys in BIND with NSEC:

ZSK: `dnssec-keygen –a RSASHA1 –b 1024 –n ZONE example.com`

KSK: `dnssec-keygen –a RSASHA1 –b 2048 –f KSK –n ZONE example.com`

And if you wanted NSEC 3….

- ZSK: `dnssec-keygen –a NSEC3RSASHA1 –b 1024 –n ZONE example.com`

- KSK: `dnssec-keygen –a NSEC3RSASHA1 –b 2048 –f KSK –n ZONE example.com`

Same required arguments, but now you have to remember how to spell NSEC3RSASHA1…

In BIND 9.7

- DNSSEC for Humans style:
- For NSEC:
  - `ZSK: dnssec-keygen example.com`
  - `KSK: dnssec-keygen –fk example.com`
- For NSEC3:
  - `ZSK: dnssec-keygen -3 example.com`
  - `KSK: dnssec-keygen -3 –fk example.com`

Smart signing

- The old way:
  - `cat *.key example.com > zone`
  - `dnssec-signzone –o example.com –k <ksk> –f example.com.signed zone <zsk>`
- The new way:
  - `dnssec-signzone –S example.com`
- Keys are imported into the zone automatically
- NSEC/NSEC3 parameters are retained when a zone is re-signed

Fully Automatic Signing of Zones

- In BIND 9.7, named can import keys from a key directory and start signing.

- The private key file format has been extended to contain key timing metadata, allowing the administrator to schedule when a key will be scheduled, published, and revoked.

Automated Trust Anchor Maintenance

- *RFC 5011, Automated Updates of DNS Security (DNSSEC) Trust Anchors*, documents a method for automated, authenticated, and authorized updating of DNSSEC "trust anchors”.

- The new managed-keys statement provides named with trusted keys which are automatically kept up to date using RFC 5011.

Simplified configuration of DLV

- A new configuration setting `auto` was added for the `dnssec-lookaside` option.
- This enables DLV by using the dlv.isc.org repository and provides a built-in key for it.
- This feature defaults to off but the key is included for ease of DLV administration.
- What is this DLV, you say?

DLV is...

- DLV (DNSSEC Look-aside Validation) is an extension to the DNSSECbis protocol. It is designed to assist in DNSSEC adoption by simplifying the configuration of recursive servers.
- DLV provides an additional entry point (besides the root zone) from which to obtain DNSSEC validation information.
- ISC hopes that as the root zone is signed, DLV is nearing the end of its usefulness, however it will remain useful and available until everyone has a chain of trust to the root zone.

Simplified DDNS Configuration

- The update-policy zone option has been extended to add a `local` setting to enable Dynamic DNS for a zone. named will generate a TSIG session key at startup which will be used for these updates.
- The nsupdate tool now has a `-l` switch to tell it to sign updates using the generated session key and to send the update requests to the localhost.
- The new ddns-confgen tool may be manually used to create a local authentication key and generate an example configuration for named.conf and the nsupdate syntax.

Why is DDNS relevant to DNSSEC?

With these new dynamic DNS features, it is also now easier to configure automatic zone re-signing for DNSSEC.

Improved and extended libdns library

The BIND 9 DNS libraries are available for use with third-party (non-BIND) applications.

BIND 9.7.0 introduces new libdns DNSSEC features including:

- DNS client API with support for DNSSEC and dynamic updates
- DNSSEC-aware `getaddrinfo()` and `getnameinfo()`

Improved Ease of Use in PKCS#11

- README.pkcs11 updated
- Added support for the AEP KeyPer HSM
- Patch to OpenSSL provides two PKCS#11 engines `sign-only` and `crypto-accelerator`
- New PKCS#11 tools for HSM operations

Improved Ease of Use in PKCS#11

- Public Key Cryptography Standard #11 (PKCS#11) defines a platform- independent API for the control of hardware security modules (HSMs) and cryptographic support devices.

- Updates in BIND 9.7:
  - README.pkcs11 updated
  - Added support for the AEP KeyPer HSM to existing support for the Sun SCA 6000 cryptographic acceleration board
  - Patch to OpenSSL provides two PKCS#11 engines `sign-only` and `crypto-accelerator`
  - New PKCS#11 tools for HSM operations:
    - `pkcs11-keygen` -- for generating RSA key pairs on the device
    - `pkcs11-list` -- for listing the PKCS#11 objects
    - `pkcs11-destroy` -- for destroying keys stored on the device

DNS rebinding attack prevention

- named can now filter responses from remote DNS servers based on addresses or CNAME/DNAME targets in the answer section.
- The new deny-answer-addresses option can reject address records if matches an ACL list. The new deny-answer-aliases option can reject CNAME aliases or DNAME names if they match a name list.
- If it matches, the answer is not cached and a SERVFAIL response is returned. This can be used to filter outside responses from returning an answer that is within your own network.

This feature is based on contributed code from Google.

attach-cache

Share view caches with new option `attach-cache`

- The new `attach-cache` option allows multiple views to share a single cache.

When configured, at named start up, it will attempt to reuse an existing cache if possible for a view to save memory and improve lookup efficiency. (It does not use previously stored cache from disk.)

How to Get BIND 9.7

BIND 9.7 Beta is now available at:
https://www.isc.org/download/software/development

If you are interested in participating in the BIND 9.7 beta program, please register at:
https://lists.isc.org/mailman/listinfo/bind-beta-response

BIND 9.7 will be publically released in December 2009.