DNSSEC Implementation Guidelines

Abstract

This paper is a brief overview of issues that ESnet sites should take into consideration when planning on implementation of DNSSEC as mandated by OMB. Only ESnet sites using the .gov domain are impacted by the mandate, but other sites may also wish to start working on DNSSEC and may find these discussions of value.

This document provides general guidance. Every site has diferent conditions and requirements and is responsible ofr determining the best course of action for each site.

1 DNSSEC Overview

DNSSEC is a mechanism to secure DNS from accepting false data by cryptographically signing DNS data. This is a critical part of preventing "man in the middle" attacks or counterfeiting data. The problem has long been known, but was not thought to be easily exploitable before the attack method discovered by Dan Kaminsky.

DNS is a hierarchical globally distributed database where data is retrieved by walking down the name tree from the root. Under the root are domains like com, net, gov, org, country codes, and others. To find the servers for any domain, you ask the parent, starting at the root. This makes a "trust anchor" method of signing data a natural fit as data must all be retrieved by walking from the root. Unlike PKI, there is no certificate authority and only a single trust point, root.

The signing uses public key cryptography when a private key, known only to the signer, creates signature DNS entries for all DNS records in the zone which can be read only with the public key. The data is not encrypted and is still available in the same way as it is today if validation is not done by the resolver. To validate a record, the public key for the data must be available and it can be found by retrieving keys from the root to the data of interest retrieving the keys from the parent zone. As long as the root is key trusted and all sub-domains between the root and the zone carrying the desired are signed, all signed records can be verified as valid.

An overview of the signing mechanism is NIST SP800-81 Rev. 1 available at:
http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-81-Rev.%201.
This is still a draft, but is close to being formally released.

2 Should I start signing DNS data?

2.1 Forward (Name to Address) zones

If your domains are in .gov, the answer is clearly 'yes'. If not, it is still 'yes'. Simple signing has NO impact on normal DNS operation. The only cost is your time and some disk space. DNSSEC is not really doing anything until you publish your keys so that validating resolvers will try to retrieve the signatures. Depending on interpretation of the mandate, publication may not be required. This interpretation may be risky.

Of the domains most commonly to be used by ESnet sites, only 'gov' and 'org' are currently signed, but plans are in the works for signing other gTLDs including .edu, .com, and .net in 2011. Several ccTLDs are signed including Brazil, Bulgaria, Thailand and Sweden. Several are close to ready to sign. The keystone of the intended operation is the signing of the root and ICANN has announced plans to have the root signed by the end of the year.

It is much simpler to use DNSSEC when your parent zone is supporting it. Otherwise the use of TARs (Trust Anchor Repositories) or the DLV (DNSSEC Look-aside Validation) must be used to make the public keys for your zone available. Due to the complications introduced by the requirements in a TAR and/or DLV system, you may want to delay the publication of any keys to allow validation until the zone's parent is signed.

2.2 Reverse zones

While reverse zones (in-addr.arpa and ip6.arpa) may be signed, signing them adds considerable computational and administrative overhead while providing much less value than the signing of the forward zones. Further, signing of reverse zones is not mandated for anyone at this time. Neither the IPv4 or IPv6 parent is currently signed, resulting in the same issues discussed in 1.1 regarding a signed path from the root to your domain. You probably do not want to sign reverse zones which are not currently being used.

3 Signing

Signing is a straight-forward operation for most zones. Zone files will grow by 5 to 20 times but disk is cheap and so is memory.

What is especially critical is "rolling" your keys. "Rolling keys" means the process of replacing old keys with new ones in a manner that does not disrupt validation of the data. It involves generating a new key, signing the data with this key (while leaving the existing key in place) and, once all cached data has expired, the signature records using the old key are removed.

Current recommendations require keys be changed monthly. There are actually two keys normally used, one to sign the data (ZSK) and the other to sign the key (KSK), but, since the update mechanisms are identical and the KSK is updated much less often, this document will stick to the ZSK.

3.1 Re-signing/rolling keys

The process of moving from old to new keys is referred to as a 'key roll'. While the key roll is technically straight-forward, the system will not tolerate errors. A failed key roll can effectively make your systems unreachable to those using validating servers. Your site is down to anyone trying to use names with broken signatures if it is not corrected prior to signature expiration! It is not trivial to recover from a failure and is always time consuming.

You can re-sign as often as you like, but the interval between signing should be short compared to the expiration of the signatures. In most cases, the data will always be signed with two keys at all times.

For example, you might sign daily (meaning signing with a new key every other day) and set the expiration to 7 days. That allows at least 5 days to fix a problem before the world goes away. If worse comes to worse, you can try to get the keys removed from your parent zone until the problem can be resolved.

4 Signing systems

There are many tools available to support signing and rolling keys. They will require substantial expertise to use properly and it is critical that they be as fully automated as possible. Both primary and backup personnel must be very familiar with features and procedures for all normal operations as well as emergency procedures needed if a key might have been compromised or a problem with the system might impact key rolls.

4.1 Do it yourself systems

OpenDNSSEC.org is working on a complete, integrated solution for DNS signing. The developers are hoping for a release in September. As with many open-source projects, unless it becomes part of a major distribution continuing support is uncertain.

The system would use PKCS #11 for key generation and access. Actual keys will be generated and validated and private keys stored either in a Hardware Security Module (HSM) or in software which emulates the function of an HSM. Such a software module is planned for the package.

OpenDNSSEC will work with a number of commercial HSMs. Prices and certifications vary widely with prices ranging from ~$1.5k to ~$24.5K.

For free tools to support software signing, see http://www.dnssec-tools.org/

While everything you need is there, it is a set of tools and not yet an integrated system.

Capabilities for managing keys and key rolls is limited in BIND, but the next release should have support for automating key rolls. This should greatly simplify "do it yourself" DNSSEC.

4.2 Hardware systems

Several vendors make DNSSEC appliances. They all can act as signing DNS servers and some can sign data transferred from any traditional server. This ability to sign data transferred from a DNS server is especially important for sites that use DNS management software or tools that cannot run on the box doing the signing. Be aware that some system that must be the master for all signed zones. Others can sign zones generated by a "hidden" master.

While expensive, hardware systems should be easy to use, highly secure, and robust. It is critical that the supplier be stable as there will certainly be updates required in the early days of DNSSEC deployment.

Hardware DNSSEC providers include Secure64 (http://www.secure64.com/automated-DNSSEC-signer-software-appliance), Xelerance (http://www.xelerance.com/appliances/), Infoblox (http://www.infoblox.com/news/dnssec.cfm), and Bluecat Networks (http://www.bluecatnetworks.com/news-events/news/114.htmll).

Infoweapons has marketed a DNSSEC appliance, but they recently withdrew from the US market.

These are presented only as a list of known providers and do not indicate any recommendation. Some of the vendors did not have a working product at the time this was written.

5 Certification

At this time there is no requirement for the certification of DNSSEC systems, but this may change in the future. FIPS 140-2 certified systems are recommended, but none of the existing systems is known to be certified at this time.

HSMs to be used with software solutions should be certified and the ones referenced by OpenDNSSEC are, though levels vary. Note that FIPS 140-1 is obsolete and you really want to look for FIPS 140-2 certification, but FIPS 140-1 certifications are still valid.

6 Operational Considerations

Staff qualified to manage the signing system need to be continuously available. That means at least two people need to be thoroughly familiar with the system and that both not be unavailable at the same time.

You should have at least two systems capable of signing the data so that you can deal with the catastrophic failure of one system. Note that you must be able to synchronize the keys between systems and this can result in complexities. Consider remote placement of the backup system so that you can re-sign data from a slave server if the site of the primary is down or off of the network for an extended period of time.

7 Testing and development

Start signing now. Until you keys are published, it will not affect the ability for retrieval of DNS data. It's a good opportunity to get experience and find out the best approach for your organization.

It also is a good idea to set up a validating resolver to familiarize yourselves and your staffs with operational use of DNSSEC. Even if the current OMB mandate does not cover some or all of your DNS, it is likely to expand over time and it is best to be ready. Even without a mandate, it is a good idea to sign zones and test systems are a safe and effective method to get experience.

As with IPv6, you should really start now.