DNSOP WG | Edward Lewis
INTERNET DRAFT | NAI Labs
Category: I-D | March 2, 2001

# Handling of DNS Zone Signing Keys
<draft-ietf-dnsop-keyhand-04.txt>

## Status of this Memo

Comments should be sent to the authors or the DNSOP WG mailing list dnsop@cafax.se.

This draft expires on September 2, 2001

## Copyright Notice

## Abstract

DNS Security Extensions require a greater interaction between zone administrations sharing a zone cut.  The center of the interaction is the handling of the zone keys of the child and the signature applied by the parent.  DNSSEC does not include a protocol for this, but the means of this interaction need definition to maintain the security of DNS.

## 1 Introduction

This document has existed for quite some time.  The purpose of this document is to capture lessons learned regarding DNSSEC zone keys.  In the past two years numerous workshops have been held, each adding to the community's lessons learned.

In past editions of this document, the outline consisted of describing the lifecycle of a key and the steps needed to get it validated by the parent. In this edition, a new approach is being taken. The lessons learned are described without regard to fitting into an operations procedure. The hope is to develop a better explanation of the issues surrounding what will someday describe a "best current practice."

## 2 Terminology

Zone keys are explicitly defined in RFC 2535, but there have been certain phrases that are increasingly used that may cause confusion to new comers.

A zone key really refers to two cryptographic values, called a public key and a private key. The two values always work in tandem, hence the singular reference. The phrase "signing with the zone key" refers to using the private key to generate digital signatures. The phrase "verifying with the zone key" refers to the use of the public key to verify the data and signature.

## 3 Threats to Keys

The threats to a zone key center on threats to the private key. There are three ways a zone key can be come useless to the owner (and possibly an advantage to an attacker). The private key could be come "exposed," "discovered," or "lost." The latter case, a lost key, refers to perhaps accidentally deleting the key from storage, and is a case that is of little concern. (Keys can be replaced easily.)

An "exposed" key refers to a private key that is seen, or copied, by an unauthorized person. This could happen if the host holding the key is infiltrated or sloppy transferring of the key (such as in unencrypted email).

A "discovered key" is one that is found through performing cryptographic analysis of the public key, data sets and signatures. Depending on various factors, such as algorithm and key size, a determined analyst can reverse engineer the private key.

This latter loss is the most troublesome. This kind of loss is what creates the limited lifetime of a key. Because of this, there is a need to fully develop key changing (or rollover) procedures.

Unfortunately, there is no current recommendation on how long it would take to discover a given private key. Such knowledge would be invaluable in the design on key handling procedures.

## 4 "Lateral Signing"

Lateral signing refers to the use of key-signing keys and data-signing keys to balance the need to change keys (avoiding discovery) and the need to configure new keys in resolvers.

This approach has been developed for the use of TLDs in absence of a signed root zone.  This approach is applicable anywhere in the DNS hierarchy, and will be needed by the root zone when it is signed.

The thought is as follows.  A zone assumes that the parent is not secured, hence must distribute a public key to all resolvers of interest.  This key is a key-signing key, it will be used to sign as little as possible to minimize the risk of discovery.  Other keys are used to sign the zone, with these keys changed roughly once a month.

At any one time, the zone's key set will have the one key-signing key and some number of data-signing keys.  The key-signing key will sign the zone key set, and the other key or keys, the zone data.

A resolver would start with the key-signing key configured.  When data arrives, it does so accompanied by a signature generated by a data-signing key.  The resolver then retrieves the data-signing key as part of the zone key set, which is signed by the key-signing key. Hence the chain is from key-signing key to data-signing key (signed by key-signing key) to data (signed by data-signing key).

The term "lateral" signing comes from the observation that the key-signing key and the data-signing key are from the same place in the hierarchy (same owner name).

## 5 Getting Validation

In order for DNSSEC to scale, zones will need to have their parents validate the zone keys.  This process is the most difficult issue facing DNSSEC deployment.

Summarizing this needed process, a child zone sends its zone key set to the parent, the parent signs it and returns the data to the child. This process is complicated by its volume (number of zones) and its repetitiveness due - to the key discovery problem.

One important issue that has been raised regarding this process is what the parent does with the child's keys once they are signed.  One school of thought is that the keys and signature are returned to the child and are forgotten by the parent.  Another school of though is that the parent retains copies of the keys and signature, perhaps even entering them into the zone file.

The former idea enables the child to "close the loop" security-wise by verifying that the parent signed the right keys.  It might be possible for an attacker to intercept the submission and modify the keys.

The latter idea leaves the parent better prepared for a key change in its zone. If the parent changes keys mid-month, or in an emergency, children zones (perhaps signed monthly) need to get the new signatures. On one workshop, this step was mishandled, resulting in the loss of many delegations.

## 6 Changing Keys

When the time comes to change a zone's keys, one issue is whether it is appropriate to retain old keys in the zone or to abruptly change the key set (with the exception of any key-signing key). The reason to retain old keys is to enable old but still valid signatures to be verified in caches. Arguments for abrupt change include the observation that this is the only way in which DNS can revoke signatures.

## 8 Size and validity period

An often-asked question is what is an appropriate key size. As mentioned earlier, a good guide is lacking. In general, per algorithm, a longer key compared to a shorter key is more difficult to discovery but takes longer to use. Longer keys can generally be used longer, but signing and verification are slower.

The period of time in which a key should be used is an unknown quantity. This will likely be a decision based upon staffing, and on a calendar basis. Once a week is likely for zones requiring tight security, once a month for others.

## 9 Random Numbers

One easily overlooked issue is the source of random numbers. A good random number generator is needed to generate truly strong keys. In the worst case, a random number generator always returning the same number would result in the same pair of keys being generated. If a zone generates a pair of keys this way and an attacker gets hold of the same key generation software, it would be possible to discover the private key simply by generating a pair of keys. This, by the way, has already been observed in workshops.

It is unfortunate that some current operating systems have poor random number generators. While this is improving, the machines used for key generation and use should be selected carefully.

## 10 Dynamic Update

Dynamic update raises an issue regarding the protection of private keys. As mentioned earlier, one threat is the exposure of the private key. This is possible of the private key is on the same machine as the name server, or even on any other reachable server. Therefore, conventional wisdom is to use non-network connected machines (perhaps behind a firewall) for all signing activity.

Dynamic update requires the server to sign data submitted to it for a zone. This means the private key must be available to the name server (on the network).

To counter this, a recommendation is offered to segregate dynamic update zones from static zones. This limits the risk to static data if a dynamic update zone key is exposed. In addition, some issues have been discovered with signed dynamic update zones, particularly the mechanism by which to refresh signatures, which also call for separating crucial static data from dynamic data.

## 11 IANA Considerations

This document does not place any requirements on the assigned numbers authority.

## 12 Security Considerations

This entire document is a note on security considerations. If the zone key is mishandled, in a way that compromises its security, then the security of its zone is compromised.

## 13 References

At some point.

## 14 Author's Address

Edward Lewis
<lewis@tislabs.com>
3060 Washington Rd (Rte 97)
Glenwood, MD 21738
+1(443)259-2352

## 15 Acknowledgements

The following individuals and groups have made significant input into the content of this document: the attendees of the NIC-SE work shop on DNSSEC, May 18 and 19, 1999, also Olafur Gudmundsson, and Brian Wellington.

A second workshop held by the CAIRN research network September 29 and 30th also provided input to this document. Dan Massey has provided input based upon this workshop and experience with DNSSEC in CAIRN.

More workshops are to be acknowledged.

## 16 Full Copyright Statement

```
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
Edward Lewis                                                NAI Labs
Phone: +1 443-259-2352                      Email: lewis@tislabs.com
```

Dilbert is an optimist.

Opinions expressed are property of my evil twin, not my employer.