Domain Name System Security WG
INTERNET DRAFT
<draft-ietf-dnssec-key-handling-00.txt>

Edward Lewis
Olafur Gudmundsson
Trusted Information Systems
November 21, 1997

Zone KEY RRSet Signing Procedure
<draft-ietf-dnssec-key-handling-00.txt>

0.0 Status of this Memo

This document is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as ``work in progress.''

To learn the current status of any Internet-Draft, please check the ``1id-abstracts.txt'' listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), ds.internic.net (US East Coast), nic.nordu.net (Europe), ftp.isi.edu (US West Coast), or munnari.oz.au (Pacific Rim).

This Internet Draft expires on 21 May 1998.

Please send comments to the authors and dns-security@tis.com.

1.0 Abstract

Under the security extensions to DNS, as defined in RFC 2065 and RFC 2137, a secured zone will have a KEY RRSet associated with the domain name at the apex of the zone. This document covers the manner in which this RRSet is generated, signed, and inserted into the name servers.

1.5 Change Log

Version 01 - draft-lewis-dnskey-handling-01.txt:

Minor editorial changes.
Added paragraph in section 3.1 elaborating on off-net versus off-net signing.
Added paragraph in section 4.0, step 2, requiring proof of private key ownership.
Added Change Log section.

Version 02 - draft-ietf-dnssec-key-handling-00.txt:
Minor editorial changes.
Dynamic update reference changed from a draft to an RFC.

2.0 Introduction

Under the security extensions to DNS, as defined in RFC 2065 [RFC2065] and [RFC2137], a secured zone will have a KEY RRSet associated with the domain name at the apex of the zone. At least one of the KEY RR's will be a public key that is used to verify SIG RR's in the zone. The SIG(KEY) RR covering this RRSet must itself be signed by some other domain name, "some other" being required to build a chain of trusted verifications. (The alternative to requiring a different signer is to have each name server hold all the public keys it will ever need in a trusted place, which is not a scaleable solution.) A key administration protocol external to the existing DNS protocol is needed to produce the signature of the KEY RR's and to get it into the DNS name servers.

As this is a first document on the subject, the "administration protocol" will be described more as an "administrative procedure or method."

The challenge is to design a secure procedure for handling the unsigned public keys as they move from the place of generation to a place where they are signed. The procedure must also eventually lead to the insertion of the keys and signature into the zone master file on a primary name server. The place of generation and the place of the signing are recommended to be disconnected from the Internet in order to protect the private keys produced and/or used in the procedure. The two locations may also be disconnected from each other.

The security of the public keys in this procedure is crucial to the operation of the secure zone. An attack in which a false public key is submitted for signing would enable a masquerade of the true zone data by the attacker.

2.1 Terminology convention

In the literature on DNS, different terms are used to describe the relationship of zones. "Super-zone and sub-zone," "parent and child," and "delegator and delegatee" each refer to two zones joined at a "zone cut." For each of the set of terms, the former is the zone above the cut point, the latter is below the cut point. In this document, we use the terms delegator and

delegatee.

3.0 DNSSEC Configuration Variants

There are a number of variants in the way in which DNSSEC can be configured that impact a discussion of key management. The discussion in section 4.0 will assume a nominal configuration (defined in section 3.4) to simplify this document. In this section, pertinent configuration decisions are described, and how the choices make a particular configuration differ from the so-called nominal configuration.

3.1 Off/On-Net Signing

In DNSSEC the configuration of DNS operations and signing fall into two categories. The most secure is the use of an "off-net" signer. The alternative is to use an "on-net" signer. These two alternatives correspond to the Mode A and Mode B distinction in UPDATE. (Mode A's initial zone signing is performed off-net.)

The decision whether off-net or on-net signing is used is based upon the risk assessment of the site's network management. An on-net key is more vulnerable to attack than an off-net key just by being present somewhere on the network. Off-net signing is recommended for tighter security. Being behind a firewall might be deemed insufficient if the administration does not trust the protection in other parts of the network. This is matter of choice for sites.

In off-net signing, the machinery performing the act of creating the keyed signature is not reachable from the network the DNS (name server set) is serving. I.e., there is no direct mechanism for data transfer from the signing machine to a name server. Without loss of generality, the DNS served network may be thought of as the Internet.

The off-net signer need not be a stand-alone machine it may be on an "air-gapped" (not physically connected) network. This network may be just a very local network (i.e., within one office or machine room), reserved for sensitive network administration use. For the purposes of this document, this will be labeled the back-room network (even if just a stand-alone machine is on it).

The back-room network needs to be able to get information from the Internet to derive the unsigned zone master files (among other things). The back-room network generates the signed

files, which are inserted to the Internet DNS servers. The mechanism to carry this out may be removable "static" media.

ADDED for draft-01:

(The preceding discussion focuses on the original signing of a zone. Dynamic update requests for both off-net and on-net situations are signed on-net, in the case of off-net, a different key is used to sign the updates. The choice of off-net or on-net is a comparison of the administrative effort to maintain off-net signing versus the risk of an on-net private-key compromise.)

For the purposes of this document, if off-net signing is used, we assume key generation is also performed off-net.

On-net signing simply means the signer is accessible over the Internet. If the back-room network exists, it is connected to

the Internet. In the procedures described below, the steps used to transfer information from the Internet to the back-room network are obviously unnecessary.

3.2 Relationship of Zone and Key Signer

In a nominal state, a zone's delegator will also be the signer of the delegated zone's KEY RR set. E.g., for a zone named "xz.test." with an NS RRSet at that name, the domain name "test." would be the delegator of "xz.test." and signer of its KEY RRSet. However, there may be cases in which some other entity is the signer.

The role and composition of the "other entity" is not yet defined, and may or may not ever be defined. This entity has been referred to as a Signing Authority, whose sole purpose is to sign records for clients. This may be more or less a certification authority for DNS KEY RRSets. For the purposes of this document, this entity will be assumed to be the delegating zone, and it will be referred to as the "signing entity."

3.3 Name Server Topology

The separation between two delegated zones may mean that the two do not share any name servers, such as most names under .COM and .COM itself. In general, the set of name servers for two zones may overlap. This document will focus on cases in which zones do not share name servers or other facilities.

If the two zones share the same name servers they likely will share the mechanism for the generation of zone keys. In this case, the transfer of information between the zones becomes a moot point because the problem may degenerate into accessing a file in a shared file system. For zones sharing a back-room network, the data for the two zones (between the off-net and on-net machines) can be transferred together.

3.4 The Nominal Configuration

The nominal configuration used within the context of this document is that the zones involved (one being the zone generating the keys and the other zone performs the signing) each employ off-line signing, and employ distinct sets of name servers. In addition, the zone performing the signing is the zone above the delegation point that creates the zone which is generating and requesting the signing of its keys.

4.0 Key Signing Protocol/Procedure

The steps described here assume the nominal configuration in section 3.4. In some configurations, the steps listed in this section may degenerate into null or very simple operations. Additionally, some steps can be carried out in parallel even with the nominal configuration, so the strict ordering described

here need not be followed.

Step 0. A delegation needs to be instituted. A means to authenticate both the delegator to the delegatee and vice versa is also needed.

A delegation may only need to be created once. A NS RRSet and a KEY RRSet must be installed by the delegating zone. Until a key pair is generated the KEY RRSet will have a null zone key, indicating that the delegated zone is initially unsecured.

Instituting means to authenticate the participants must occur initially, and then again if the means of authentication (e.g., a secret key) is ever compromised.

How a delegation comes about is a subject for registries and/or local network administration policies and procedures. These groups should be aware of the responsibilities entailed in instituting DNS security, especially the need for an active recurring relationship, as the remaining steps describe.

It is assumed that at some point, the delegated zone acquires a

trusted public key(s) for at least one other entity. This could be for root, the delegating zone, or for a signing authority. These keys may be DNS zone keys or keys for some application, e.g., trusted mail. This will enable the use of other secure services to achieve the following steps. Selecting the services may be within the scope of this document, but which should be selected is still open for discussion.

Step 1. Delegated zone generates zone keys. A new pair may be generated without changing the other pairs in use (assuming others exist).

Step 2. The delegated zone sends keys to the signing entity. All of the public key information, encoded in such a way that the KEY RR's can be generated from it, crosses from the back-room net to the Internet, and is shipped securely to the signing entity. (Implementing "securely" is still an open issue.) It is important that both the delegated zone and the signing entity authenticate themselves to each other.

All public keys must be included, both newly generated and those in current use. Keys are retired through omission.

ADDED for draft-01:

The delegated zone must prove ownership of the private keys corresponding to each public key. This may be done by signing the collection of public key data with each of the private keys. Thus the submission would consist of one copy of each public key and as many signatures as there were public keys. (For example, submitting five public keys would require sending all five plus five signatures.) This signing is only done to prove the

ownership of the private key, not for authentication.

Step 3. The signing entity signs the key set. The algorithm used to sign the KEY RRSet need not be the same as the algorithm(s) for which the keys were generated.

Step 4. The delegated zone receives KEY RRSet and SIG(KEY) RR from the signing entity. The delegated zone must verify the keys and signature locally. The zone must also verify that the KEY RRSet is identical to the set of keys submitted for signature in step 2, to protect against a masquerader from submitting keys for signature. Once the records are signed, there is no requirement for enhanced security while transmitting the information across the Internet because the DNS signature provides non-repudiation.

Step 5. Delegating zone gets the KEY RRSet and SIG(KEY) RR. The KEY RRSet and the SIG(KEY) RR are sent from the signing entity to the delegating zone's master files and optionally the name servers. In the nominal case, the signing entity and the delegating zone are one in the same, so this may be a trivial step. (The latter is to ensure the public key will be available for verifications once the signing process - step 7 - is finished.)

Step 6. The delegating zone signs its zone data. This step may be done in parallel with steps 2-5. Note: signing a zone does not require that a new key pair be generated.

Step 7. The new zone data enters DNS. The KEY RRSet, SIG(KEY RR) and the rest of the signed zone data and signatures traverse from the back-room network and are inserted into the DNS primary name server serving the Internet side.

Steps 1 through 7 are repeated whenever a new key pair is required. Note that the signing in step 6 may not sign all records; some records may have signature records from older keys that are sufficient.

5.0 Resigning a KEY RRSet

When the delegating zone resigns itself, the KEY RRSet of a delegated zone may be resigned. In this case, the newly created SIG(RR) must be sent to the delegatee for inclusion.

The signing of a delegatee's keys in the manner of the previous paragraph may be prompted by a request from the delegatee. A SIG(RR) record may be approaching its expiration date, although the KEY RRSet it is verifying has not changed.

6.0 Open Issues

This section is intentionally left undeveloped to encourage more feedback.

Timing of steps, required response times.

The signing cycles of zones will likely be out of phase of each other. If they were not, then there would be "signing crunches" which would add variability to the spacing of events in the procedure. One issue is how this should be addressed. Should there be a recommended limit on signing entity's response?

Should this even be specified?

Can secure e-mail be used? Perhaps, and discussions to this effect have occurred, using secure e-mail as a conduit for (at least) the unsigned keys.

7.0 Operational Considerations

A widely delegated zone, such as .COM, or a zone publishing KEY RR's for others, such as a large Internet access provider, should expect a huge performance impact in signing the KEY RRSets for it delegations. Running on a Pentium 166MHz computer, simply signing the current .COM records, requires 40 hours. (Measured in January 1997.) This covers just the NXT RRSets and a few other records. Having to sign a KEY RRSet for each member of the zone will require about the same computing resources, and much more overhead in the handling of the individual KEY RRSets.

8.0 Security Considerations

This document discusses a procedure for handling the keys used by DNS for its security and the keys for applications employing DNS for key distribution. Once in DNS, keys are protected by the presence of a keyed hash, which can be used to verify the source and integrity of the public key data. During the process described here, the keyed hash is not yet present, leaving the keys vulnerable to modification. The security of this process is crucial to the usefulness of DNS as a key distribution mechanism. At this point many issue remain to be resolved, a thorough security analysis of the process is premature.

9.0 References

[RFC2065] "Domain Name System Security Extensions," D. Eastlake, 3rd, and C. Kaufman
http://ds.internic.net/rfc/rfc2065.txt

[RFC2137] "Secure Domain Name System Dynamic Update," D. Eastlake, 3rd
http://ds.internic.net/rfc/rfc2137.txt

10.0 Author's Addresses

Edward Lewis
Trusted Information Systems
3060 Washington Road
Glenwood, MD 21738
+1 301 854 5794
<lewis@tis.com>

Olafur Gudmundsson
Trusted Information Systems
3060 Washington Road
Glenwood, MD 21738
+1 301 854 5700
<ogud@tis.com>