Secure Domain Name System (DNS) Dynamic Update
------ ------ ---- ------ ----- ------- ------

Status of This Document

Abstract

   Revised Domain Name System (DNS) protocol extensions to authenticate
   the data in DNS and provide key distribution services have been
   defined in draft-ietf-dnssec-secext2-*.txt, which obsoletes the
   original DNS security protocol definition in RFC 2065. In addition,
   symetric key DNS transaction signatures have been defined in draft-
   ietf-dnsind-tsig-*.txt. Secure DNS Dynamic Update operations were
   also been defined [RFC 2137] in connection RFC 2065. This document
   updates secure dynamic update in light of draft-ietf-dnssec-secext2-
   .txt and draft-ietf-dnsind-tsig-.txt. It describes how to use
   digital signatures covering requests and data to secure updates and
   restrict updates to those authorized to perform them as indicated by
   the updater's possession of cryptographic keys.

Table of Contents

[1](#). Introduction

Dynamic update operations have been defined for the Domain Name
System (DNS) in [RFC 2136](#) but that RFC does not include a description
of security for those updates. Public key means of securing DNS data
and transactions and using it for public key distribution were
defined in [RFC 2065](#) which has been updated by [draft-ietf-dnssec-sexect2](#)-*.txt, and secret key means of securing DNS transactions are
defined in [draft-ietf-dnsind-tsig](#)-*.txt.

This document provides techniques based on the updated DNS security
RFC [draft-ietf-dnssec-sexect2](#)-*.txt and [draft-ietf-dnsind-tsig](#)-*.txt
to authenticate DNS updates of secure zones. (Secret key signatures
could be used to authenticate updates on non-secured DNS zones. That
case In not considered in this document.)

Familiarity with the DNS system [RFC 1034, 1035] is assumed.
Familiarity with the DNS security and dynamic update will be helpful.

[1.1](#). Overview of DNS Dynamic Update

DNS dynamic update defines a new DNS opcode, new DNS request and
response structure if that opcode is used, and new error codes. An
update can specify complex combinations of deletion and insertion
(with or without pre-existence testing) of resource records (RRs)
with one or more owner names; however, all testing and changes for
any particular DNS update request are restricted to a single zone.
Updates occur at the primary server for a zone.

The primary server for a dynamic zone must increment the zone SOA
serial number when an update occurs or the next time the SOA is
retrieved if one or more updates have occurred since the previous SOA
retrieval and the updates themselves did not update the SOA.

[1.2](#). Overview of Public Key DNS Security

DNS security authenticates data in the DNS by also storing digital
signatures in the DNS as SIG resource records (RRs). A SIG RR
provides a digital signature on the set of all RRs with the same
owner name and class as the SIG and whose type is the type covered by
the SIG. The SIG RR cryptographically binds the covered RR set to
the signer, signature inception and expiration date, etc. There are
one or more keys associated with every secure zone and all data in
the secure zone is signed either by a zone key or by a dynamic update
key tracing its authority to a zone key.

DNS security also defines transaction SIGs and request SIGs.

Transaction SIGs appear at the end of a response. They authenticate
the response and bind it to the corresponding request using the key
of the host where the responding DNS server is.

Request SIGs appear at the end of a request and authenticate the
request with the key of the submitting entity.

DNS security also permits the storage of public keys in the DNS via
KEY RRs. These KEY RRs are also, of course, authenticated by SIG
RRs. KEY RRs for zones may be stored in their superzone and/or their
authoritive subzone servers so that the secure DNS tree of zones can
be traversed by a security aware resolver.

1.3 Overview of Secret Key DNS Security

draft-ietf-dnsind-tsig-*.txt provides a means for two processes that
share a secret key to authenticate DNS requests and responses sent
between them by appending TSIG digital signature RRs to those
requests and responses. Secret key digital signatures are generally
much faster to calculate and verify than public key digital
signatures. In addition, the need, in general, to cache KEY RRs and
perform the KEY-SIG chain verifications is avoided.

However, the cost for this speed and simplicity in TSIG use is the
requirement to securely achieve key distribution or agreement between
the communicating processes and to achieve agreement as to the
authority represented by a correct TSIG on a requested using a
partciular key.

[2](#). **Two Basic Modes**

   A dynamic secure zone is any secure DNS zone that
      (1) has a zone KEY RR signatory field indicates that updates are
          implemented and either
      (2a) contains one or more KEY RRs that can authorize dynamic
          updates, i.e., entity or user KEY RRs with the signatory field
          non-zero, or
      (2b) has a primary server with one or more secret keys configured
          to authorize updates requests and shared with one or more
          update requesters.

   Note: 2a and 2b can both be true for a zone.

   There are two basic modes of dynamic secure zone which relate to the
   update strategy, mode A and mode B. A summary comparison table is
   given below and then each mode is described.

                  SUMMARY OF DYNAMIC SECURE ZONE MODES

   CRITERIA: | MODE A | MODE B
   =========================+===================+===================
   Definition: | Zone Key Off line | Zone Key On line
   =========================+===================+===================
   Server Workload | Medium | High
   -------------------------+-------------------+-------------------
   Key Restrictions | Fine grain | Coarse grain
   -------------------------+-------------------+-------------------
   Dynamic Data Temporality | Transient | Permanent
   -------------------------+-------------------+-------------------
   Dynamic Key Rollover | No | Yes
   -------------------------+-------------------+-------------------

   NOTE: The Mode A / Mode B distinction only effects the validation
   and performance of update requests. It has no effect on retrievals.

[2.1](#). **Mode A**

   For mode A, the zone owner private key and static zone master file
   are kept off-line for maximum security of the static zone contents.

   As a consequence, any dynamicly added or changed RRs are signed in
   the secure zone by their authorizing dynamic update key and they are
   backed up, along with this SIG RR, in a separate online dynamic
   master file. In this type of zone, server computation is generally
   reduced since the server need only check signatures on the update
   data and request, which have already been signed by the updater

(generally a much faster operation than signing data) and update the

NXT RRs which need to be changed, if any. Because the dynamicly
added RRs retain their update KEY signed SIG, finer grained control
of updates can be implemented via the KEY RR signatory field (unique
name restriction and weak update key restriction). Because dynamic
data is only stored in the online dynamic master file and only
authenticated by dynamic keys which expire, updates are transient in
nature. Key rollover for an entity that can authorize dynamic
updates is more cumbersome since the authority of their key must be
traceable to a zone key and so, in general, they must securely
communicate a new key to the zone authority for manual transfer to
the off line static master file. NOTE: for this mode the zone SOA and
NXT RRs must be signed by a dynamic update key, which will be an end
entity key with an owner name of the zone name, and that private key
must be kept on line so that the SOA and NXTs can be changed for
updates.

2.2. Mode B

For mode B, the zone owner private key and master file are kept on-
line at the zone primary server. When authenticated updates succeed,
SIGs under the zone key for the resulting data (as well as possible
NXT and SOA changes) are calculated and these SIG (and possible
SOA/NXT) changes are entered into the zone and the unified on-line
master file.

As a consequence, this mode generally requires more computational
effort on the part of the server as it computes zone data signatures
in addition to verifying the signatures on requests. Because signing
generally takes more effort than verification, these signatures
generally will take more effort to calculate than it would take to
verify the data signatures required in Mode A. Because the zone key
is used to sign all the zone data, the information as to who
originated the current state of dynamic RR sets and even that data is
the result of a dynamic update as opposed to coming from an original
master file, is lost, making unavailable the fine grain control of
some values of the KEY RR signatory field. In addition, the
incorporation of the updates into the primary master file and their
authentication by the zone key makes them permanent in nature.
Maintaining the zone key on-line also means that dynamic update keys
which are signed by the zone key can be dynamically updated in real
time since the zone key is available to dynamically sign new values.

3. Keys

Dynamic update requests depend on update keys as described in section 3.1 below. In addition, the zone secure dynamic update mode and availability of some options is indicated in the zone KEY(s). Finally, a special rule is used in searching for KEYs to validate updates as described in section 3.3.

3.1. Update Keys

All update requests to a secure zone must include signature(s) by one or more private or secret keys that together can authorize that update. In order for the Domain Name System (DNS) server executing the update request to confirm this (1) any secret keys must be know to it, along with the authority represented by the secret key, and (2) any private key or keys must have the corresponding public key or keys available to and authenticatable by that server as specially flagged KEY Resource Records (RRs).

The scope of authority of any secret keys is as configured at the Server. Methods of describing and configuring such authority are not discussed in this document.

The scope of authority of public update keys is indicated by their KEY RR owner name, class, and signatory field flags as described below. In addition, such KEY RRs MUST be entity or user keys and not have the authentication use prohibited bit on.

All parts of the actual update MUST be within the scope/authority of at least one of the keys used for a request SIG or TSIG on the update request as described in section 4.

3.1.1. Public Update Key Name Scope

The owner name of any update authorizing KEY RR must (1) be the same as the owner name of any RRs being added or deleted or (2) a wildcard name including within its extended scope (see section 3.3) the name of any RRs being added or deleted and those RRs must be in the same zone.

3.1.2. Public Update Key Class Scope

The class of any update authorizing KEY RR must be the same as the

class of any RR's being added or deleted.

3.1.3. Public Update Key Signatory Field

The four bit "signatory field" (see draft-ietf-dnssec-secext2-*.txt)
of any update authorizing KEY RR must be non-zero. The bits have the
meanings described below for non-zone keys (see section 3.2 for zone
type keys).

```
        UPDATE KEY RR SIGNATORY FIELD BITS

       0           1           2           3
 +-----------+-----------+-----------+-----------+
 |   zone    |  strong   |  unique   |  general  |
 +-----------+-----------+-----------+-----------+
```

Bit 0, zone control - If nonzero, this key is authorized to attach,
     detach, and move zones by creating and deleting NS, glue A, and
     zone KEY RR(s). If zero, the key can not authorize any update
     that would effect such RRs. This bit is meaningful for both
     type A and type B dynamic secure zones. An update attempting to
     add an NS or zone KEY RR to a node (i.e., make the node a
     delegation point) is illegal if there are any deeper nodes in
     the zone.

     NOTE: do not confuse the "zone" signatory field bit with the
     "zone" key type bit.

Bit 1, strong update - If zero, the key can only authorize updates
     where any existing RRs of the same owner and class are
     authenticated by a SIG using the same key. If nonzero, this key
     is authorized to add and delete RRs even if there are other RRs
     with the same owner name and class that are authenticated by a
     SIG signed with a different dynamic update KEY. This bit is
     meaningful only for type A dynamic zones that have a zone KEY
     advertising that the feature is available. It is ignored in
     type B dynamic zones.

     Keeping this bit zero on multiple KEY RRs with the same or
     nested wild card owner names permits multiple entities to exist
     that can create and delete names but can not effect RRs with
     different owner names from any they created. In effect, this
     creates two levels of dynamic update key, strong and weak, where
     weak keys are prohibited from interfering with each other but a
     strong key can interfere with any weak keys or other strong
     keys.

Bit 2, unique name update - This bit is useful only if the owner name
     is a wildcard. (Any dynamic update KEY with a non-wildcard name
     is, in effect, a unique name update key.) If zero, this key is
     authorized to add and updates RRs for any number of names within

its wildcard scope. If nonzero, this key is authorized to add

and update RRs for only a single owner name. If there already
exist RRs with one or more names signed by this key, they may be
updated but no new name created until the number of existing
names is reduced to zero. This bit is meaningful only for mode
A dynamic zones that have a zone KEY advertising that the
feature is available. It is ignored in mode B dynamic zones.

This bit can be used to restrict a KEY from flooding a zone with
new names. In conjunction with a local administratively imposed
limit on the number of dynamic RRs with a particular name, it
can completely restrict a KEY from flooding a zone with RRs.

Bit 3, general update - The general update signatory field bit has no
special meaning. If the other three bits are all zero, it must
be one so that the field is non-zero to designate that the key
is an update key. The meaning of all values of the signatory
field with the general bit on and one or more other signatory
field bits on is reserved.

All the signatory bit update authorizations described above only
apply if the update is within the name and class scope as per
sections 3.1.1 and 3.1.2.

3.2. Zone Keys and Update Modes

Zone type keys are automatically authorized to sign anything in their
zone, of course, regardless of the value of their signatory field.
For zone keys, the signatory field bits have different means than
they they do for update keys, as shown below. The signatory field
MUST be zero if dynamic update is not supported for a secure zone and
MUST be non-zero if it is.


```
        ZONE KEY RR SIGNATORY FIELD BITS

      0           1           2           3
+-----------+-----------+-----------+-----------+
|   mode    |   strong  |   unique  |  general  |
+-----------+-----------+-----------+-----------+
```

Bit 0, mode - This bit indicates the update mode for this zone. Zero
indicates mode A while a one indicates mode B.

Bit 1, strong update - If nonzero, this indicates that the "strong"
key feature described in section 3.1.3 above is implemented and
enabled for this secure zone. If zero, the feature is not
available and all update keys are treated as strong. Has no

effect if the zone is a mode B secure update zone.

Bit 2, unique name update - If nonzero, this indicates that the
     "unique name" feature described in section 3.1.3 above is
     implemented and enabled for this secure zone. If zero, this
     feature is not available and no wildcard update key is treated
     as restricted to a single name. Has no effect if the zone is a
     mode B secure update zone.

Bit 3, general - This bit has no special meaning. If dynamic update
     for a zone is supported and the other bits in the zone key
     signatory field are zero, it must be a one. The meaning of zone
     keys where the signatory field has the general bit and one or
     more other bits on is reserved.

If there are multiple zone KEY RRs with non-zero signatory fields and
zone policy is in transition, they might have different signatory
field values. In that case, strong and unique name restrictions MUST
be enforced as long as there is a non-expired zone key being
advertised that indicates mode A with the strong or unique name bit
on respectively. Mode B updates (i.e., no data signatures) MUST be
supported as long as there is a non-expired zone key that indicates
mode B. Mode A or mode ambiguous updates may be treated as mode B
updates at server option if non-expired zone keys indicate that both
are supported.

A server that will be executing update operations on a zone, that is,
the primary master server, MUST NOT advertize a zone key that will
attract requests for a mode or features that it can not support.

3.3. Wildcard Public Key Punch Through

Just as a zone key is valid throughout the entire zone, public update
keys with wildcard names are valid throughout their extended scope,
within the zone. That is, they remain valid for any name that would
match them, even existing specific names within their apparent scope.

(If this were not so, then whenever a name within a wildcard scope
was created by dynamic update using a wildcard named public update
key for authorization, it would be necessary to first create a copy
of the KEY RR with this name, because otherwise the existence of the
more specific name would hide the authorizing KEY RR and would make
later updates impossible. An updater could create such a KEY RR but
could not zone sign it with their authorizing signer. They would
have to sign it with the same key using the wildcard name as signer.
(This would create update KEYs signed by update KEYs which was
permitted in RFC 2065 but, for simplicity, is prohibit in draft-
ietf-dnssec-secext2-*.txt which requires all KEYs to be signed by
zone keys.) Thus in creating, for example, one hundred type A RRs

authorized by a *.1.1.1.in-addr.arpa KEY RR, without key punch

through 100 As, 100 KEYs, and 200 SIGs would have to be created as
opposed to merely 100 As and 100 SIGs with wildcard key punch
through.)

4. Update Signatures

   Two kinds of signatures can appear in updates. Request signatures,
   which are always required, cover the entire request and authenticate
   the DNS header, including opcode, counts, etc., as well as the data.
   Data signatures, on the other hand, appear only among the RRs to be
   added and are only required for mode A operation. These two types of
   signatures are described further below.

4.1. Update Request Signatures

   An update can effect multiple owner names in a zone. It may be that
   these different names are covered by different public or secret
   dynamic update keys. For every owner name effected, the updater must
   know a private or secret key valid to authorize updates for that name
   (and the zone's class) and must prove this by appending request SIG
   and/or TSIG RRs under each such key.

   Request signatures occur in the Additional Information section. As
   specified in draft-ietf-dnssec-secext2-*.txt, a public request
   signature is a SIG RR occurring at the end of a request with a type
   covered field of zero. As specified in draft-ietf-dnsind-tsig-*.txt,
   a secret key request signature is a TSIG RR occuring at the end of
   the request. Each request SIG or TSIG signs the entire request,
   including DNS header, but excluding any other request signatures and
   with the ARCOUNT in the DNS header set to what it would be without
   the request signatures.

4.2. Update Data Signatures

   Mode A dynamic secure zones require that the update requester provide
   SIG RRs that will authenticate the after-update state of all RR sets
   that are changed by the update and are non-empty after the update.
   These SIG RRs appear in the request as RRs to be added and the
   request must delete any previous data SIG RRs that are invalidated by
   the request.

   In Mode B dynamic secure zones, all zone data is authenticated by
   zone key SIG RRs. In this case, data signatures need not be included
   with the update. A prospective updater can determine which mode an
   updatable secure zone is using by examining the signatory field bits
   of the zone KEY RR or RRs (see section 3.2).

5. Security Considerations

   Any secure zone permitting dynamic updates is inherently less secure
   than a static secure zone maintained off line as recommended in
   draft-ietf-dnssec-secops-*.txt. If nothing else, secure dynamic
   update requires on line change to and re-signing of the zone SOA
   resource record (RR) to increase the SOA serial number. This means
   that compromise of the primary server host could lead to arbitrary
   serial number changes.

   Isolation of dynamic RRs to separate zones from those holding most
   static RRs can limit the damage that could occur from breach of a
   dynamic zone's security.

6. IANA Considerations

   Allocations of values of the KEY RR Signatory field described herein
   as "reserved" requires an IETF consensus.

References

   [RFC1035] - Domain Names - Implementation and Specifications, P.
   Mockapetris, November 1987.

   [RFC1034] - Domain Names - Concepts and Facilities, P. Mockapetris,
   November 1987.

   [RFC2065] - Domain Name System Security Extensions. D. Eastlake, 3rd,
   C. Kaufman. January 1997

   [RFC2136] - Dynamic Updates in the Domain Name System (DNS UPDATE).
   P. Vixie, Ed., S. Thomson, Y. Rekhter, J. Bound. April 1997.

   [RFC2137] - Secure Domain Name System Dynamic Update. D. Eastlake.
   April 1997.

   draft-ietf-dnsind-tsig-*.txt

   draft-ietf-dnssec-secext2-*.txt.

   draft-ietf-dnssec-secops-*.txt.

Author's Address

   Donald E. Eastlake, 3rd
   Transfinite Systems Company
   318 Acton Street
   Carlisle, MA 01741 USA

   Telephone: +1 978-287-4877
                 +1 978-371-7148 (fax)
   email: dee3@torque.pothole.com

Expiration and File Name

   This draft expires February 1999.

   Its file name is draft-ietf-dnssec-update2-00.txt.