Secure Domain Name System Dynamic Update

Status of this Memo

   This document specifies an Internet standards track protocol for the
   Internet community, and requests discussion and suggestions for
   improvements. Please refer to the current edition of the "Internet
   Official Protocol Standards" (STD 1) for the standardization state
   and status of this protocol. Distribution of this memo is unlimited.

Abstract

   Domain Name System (DNS) protocol extensions have been defined to
   authenticate the data in DNS and provide key distribution services
   [RFC2065]. DNS Dynamic Update operations have also been defined
   [RFC2136], but without a detailed description of security for the
   update operation. This memo describes how to use DNSSEC 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 without a detailed description of
   security for those updates. Means of securing the DNS and using it
   for key distribution have been defined in RFC 2065.

   This memo proposes techniques based on the defined DNS security
   mechanisms to authenticate DNS updates.

   Familiarity with the DNS system [RFC 1034, 1035] is assumed.
   Familiarity with the DNS security and dynamic update proposals 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 secure 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 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, time signed, signature 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. Transaction SIGs
authenticate the response and bind it to the corresponding request
with 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.

Request SIGs are the primary means of authenticating update requests.

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 are stored in their superzone and subzone
servers, if any, so that the secure DNS tree of zones can be
traversed by a security aware resolver.

2. Two Basic Modes

A dynamic secure zone is any secure DNS zone containing one or more
KEY RRs that can authorize dynamic updates, i.e., entity or user KEY
RRs with the signatory field non-zero, and whose zone KEY RR
signatory field indicates that updates are implemented. 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	Low	High
Static Data Security	Very High	Medium-High
Dynamic Data Security	Medium	Medium-High
Key Restrictions	Fine grain	Coarse grain
Dynamic Data Temporality	Transient	Permanent
Dynamic Key Rollover	No	Yes

For mode A, the zone owner key and static zone master file are always
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 minimized
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. However, the AXFR SIG and
NXT RRs which covers the zone under the zone key will not cover
dynamically added data. Thus, for type A dynamic secure zones, zone
transfer security is not automatically provided for dynamically added
RRs, where they could be omitted, and authentication is not provided
for the server denial of the existence of a dynamically added type.
Because the dynamicly added RRs retain their update KEY signed SIG,
finer grained control of updates can be implemented via bits in the
KEY RR signatory field. 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 must be signed by a dynamic update
key and that private key must be kept on line so that the SOA can be
changed for updates.

For mode B, the zone owner 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 (including the possible NXT
type bit map changes) are calculated and these SIG (and possible NXT)
changes are entered into the zone and the unified on-line master
file. (The zone transfer AXFR SIG may be recalculated for each
update or on demand when a zone transfer is requested and it is out
of date.)

As a consequence, this mode requires considerably more computational
effort on the part of the server as the public/private keys are
generally arranged so that signing (calculating a SIG) is more effort
than verifying a signature. The security of static data in the zone
is decreased because the ultimate state of the static data being
served and the ultimate zone authority private key are all on-line on
the net. This means that if the primary server is subverted, false
data could be authenticated to secondaries and other
servers/resolvers. On the other hand, this mode of operation means
that data added dynamically is more secure than in mode A. Dynamic
data will be covered by the AXFR SIG and thus always protected during
zone transfers and will be included in NXT RRs so that it can be
falsely denied by a server only to the same extent that static data
can (i.e., if it is within a wild card scope). 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 is lost, making
unavailable the effects of some of the update control bits in 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 then 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 since the zone key is available to
dynamically sign new values.

NOTE: The Mode A / Mode B distinction only effects the validation
and performance of update requests. It has no effect on retrievals.
One reasonable operational scheme may be to keep a mostly static main
zone operating in Mode A and have one or more dynamic subzones
operating in Mode B.

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. 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 signatures by one
   or more key(s) that together can authorize that update. In order for
   the Domain Name System (DNS) server receiving the request to confirm
   this, the key or keys must be available to and authenticated by that
   server as a specially flagged KEY Resource Record.

   The scope of authority of such 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 of at least one of the keys used for a
   request SIG on the update request as described in section 4.

3.1.1 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 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 Update Key Signatory Field

   The four bit "signatory field" (see RFC 2065) 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.

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

     Bit 1, strong update - 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. 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. This bit
          is meaningful only for type A dynamic zones and 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 limited in interfering with each other but a
          strong key can interfere with any weak keys or other strong
          keys.

     Bit 2, unique name update - 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 and is ignored in mode B dynamic zones. This bit
          is meaningful 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.)

          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 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 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. 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. Has no effect if the zone is a mode B
        secure update zone.

   Bit 3, general - This bit has no special meeting. 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 dynamic update KEY RRs for a zone and zone
   policy is in transition, they might have different non-zero signatory
   fields. 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 MUST be supported as long as there is a
   non-expired zone key that indicates mode B. Mode A 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 advertise a zone key that will
attract requests for a mode or features that it can not support.

3.3 Wildcard Key Punch Through

Just as a zone key is valid throughout the entire zone, 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, 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.
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 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 dynamic update keys.
For every owner name effected, the updater must know a private key
valid for that name (and the zone's class) and must prove this by
appending request SIG RRs under each such key.

As specified in RFC 2065, a request signature is a SIG RR occurring
at the end of a request with a type covered field of zero. For an
update, request signatures occur in the Additional information
section. Each request SIG signs the entire request, including DNS
header, but excluding any other request SIG(s) and with the ARCOUNT
in the DNS header set to what it wold be without the request SIGs.

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 resolver can determine which mode an updatable
   secure zone is using by examining the signatory field bits of the
   zone KEY RR (see section 3.2).

5. Security Considerations

   Any zone permitting dynamic updates is inherently less secure than a
   static secure zone maintained off line as recommended in RFC 2065. 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.

References

   [RFC2065] Eastlake, D., and C. Kaufman, "Domain Name System Security
   Extensions", RFC 2065, CyberCash, Iris, January 1997.

   [RFC2136] Vixie, P., Editor, Thomson, T., Rekhter, Y., and J. Bound,
   "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136,
   April 1997.

   [RFC1035] Mockapetris, P., "Domain Names - Implementation and
   Specifications", STD 13, RFC 1035, November 1987.

   [RFC1034] Mockapetris, P., "Domain Names - Concepts and Facilities",
   STD 13, RFC 1034, November 1987.

Author's Address

   Donald E. Eastlake, 3rd
   CyberCash, Inc.
   318 Acton Street
   Carlisle, MA 01741 USA

   Phone: +1 508-287-4877
             +1 508-371-7148 (fax)
             +1 703-620-4200 (main office, Reston, Virginia, USA)
   EMail: dee@cybercash.com