DNSSEC Working Group Brian Wellington (TISLabs)
INTERNET-DRAFT February 1999

<draft-ietf-dnssec-simple-update-01.txt>

Updates: RFC 2065, RFC 2136, [TSIG]
Replaces: RFC 2137, [update2]

Simple Secure Domain Name System (DNS) Dynamic Update

Status of this Memo

Abstract

This draft proposes an alternative method for performing secure Domain Name System (DNS) dynamic updates. The method described here is both simple and flexible enough to represent any policy decisions. Secure communication based on request/transaction signatures [TSIG] is used to provide authentication and authorization.

1 - Introduction

Dynamic update operations for the Domain Name System are defined in [RFC2136], but no mechanisms for security have been defined. Request and transaction signatures are defined in [TSIG].

Familiarity with the DNS system [RFC1034, RFC1035] as well as the proposals mentioned above is assumed. Familiarity with DNS Security [RFC2065, secext2] is assumed in section (4).

1.1 - Overview of DNS Dynamic Update

DNS dynamic update defines a new DNS opcode and a new interpretation of the DNS message if that opcode is used. An update can specify insertions or deletions of data, along with prerequisites necessary for the updates to occur. All tests and changes for a DNS update request are restricted to a single zone, and are performed at the primary server for the zone. The primary server for a dynamic zone must increment the zone SOA serial number when an update occurs or before the next retrieval of the SOA.

1.2 - Overview of DNS Transaction Security

[TSIG] provides a means for two processes that share a secret key to authenticate DNS requests and responses sent between them. This is done by appending TSIG digital signature (keyed hash) RRs to those messages. Keyed hashes are simple to calculate and verify, and do not require caching of data.

2 - Authentication

TSIG records are attached to all secure dynamic update messages. This allows the server to verifiably determine the originator of the message. It can then use this information in the decision of whether to accept the update. DNSSEC SIG records may be included in an update message, but MAY NOT be used for authentication purposes in the update protocol. If a message fails the authentication test due to an unauthorized key, the failure is indicated with the REFUSED rcode. Other TSIG or dynamic update errors are returned unchanged.

3 - Policy

All policy is dictated by the server and is configurable by the zone administrator. The server's policy defines criteria which determine if the key used to sign the update is permitted to update the records requested. By default, a key cannot make any changes to the zone; the key's scope must be explicitly enabled. There are several reasons that this process is implemented in the server and not the protocol (as in [RFC2137, update2], where the signatory bits of KEY records may define the policy).

3.1 - Flexibility

Storing policy in the signatory fields of DNS keys is overly restrictive. Only a fixed number of bits are present, which means that only a fixed number of policy decisions are representable. There are many decisions that do not fit into the framework imposed by the signatory field; a zone administrator cannot effectively impose a policy not implemented in the draft defining the field.

There may be any number of policies applied in the process of authorization, and there are no restrictions on the scope of these policies. Implementation of the policies is beyond the scope of this document.

3.2 - Simplicity

Policy decisions in the server could be used as an adjunct to policy fields in the KEY records. This could lead to confusion if the policies are inconsistent. Furthermore, since there is no need to expose policies, a central configuration point is more logical.

3.3 - Extendibility

If a policy is changed, there are no changes made to the DNS protocol or the data on the wire. This means that new policies can be defined at any point without adverse effects or interoperability concerns.

4 - Interaction with DNSSEC

A successful update request may or may not include SIG records for each RRset. Since SIG records are not used for authentication in this protocol, they are not required. If the updated zone is signed, the server will generate SIG records for each incoming RRset with the Zone key (which MUST be online). If there are any non-DNSSEC SIG records present, they are retained. If there are SIG records that have been generated by the appropriate zone KEY, these SIGs are verified and retained if the verification is successful. DNSSEC SIG records generated by other KEYs are dropped. The server will generate SIG records for each set with the Zone key, unless one has already been verified. The server will also generate a new SOA record and possibly new NXT records, and sign these with the Zone key.

The server MUST update the SOA record and MAY generate new NXT records when an update is received. Unlike traditional dynamic update, the client is forbidden from updating SOA 1 NXT records.

5 - Security considerations

For a secure zone to support dynamic update, the Zone key MUST be online (unlike [RFC2137]). No additional protection is offered by having the Zone key offline and an Update key online, since compromising any key that can sign the zone's data compromises the zone itself.

6 - References

[RFC1034] P. Mockapetris, ``Domain Names - Concepts and Facilities,'' RFC 1034, ISI, November 1987.

[RFC1035] P. Mockapetris, ``Domain Names - Implementation and Specification,'' RFC 1035, ISI, November 1987.

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

[RFC2136] P. Vixie (Ed.), S. Thomson, Y. Rekhter, J. Bound ``Dynamic Updates in the Domain Name System,'' RFC 2136, ISC & Bellcore & Cisco & DEC, April 1997.

[RFC2137] D. Eastlake ``Secure Domain Name System Dynamic Update,'' RFC 2137, CyberCash, April 1997.

[secext2] D. Eastlake ``Domain Name System Security Extensions,'' draft-ietf-dnssec-secext2-07.txt, IBM, December 1998.

[TSIG] P. Vixie (ed), O. Gudmundsson, D. Eastlake, B. Wellington ``Secret Key Transaction Signatures for DNS (TSIG),'' draft-ietf-dnsind-tsig-08.txt, ISC & TISLabs & IBM & TISLabs, February 1999.

[update2] D. Eastlake ``Secure Domain Name System (DNS) Dynamic Update,'' draft-ietf-dnssec-update2-00.txt, Transfinite Systems Company, August 1998.

7 - Author's Address

Brian Wellington
TISLabs at Network Associates
3060 Washington Road, Route 97
Glenwood, MD 21738
+1 443 259 2369
<bwelling@tislabs.com>