Status of This Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on January 1, 2010.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (http://trustee.ietf.org/license-info). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Abstract

When DNS validators have trusted keys, but have been offline for a longer period, key rollover will fail and they are stuck with stale trust anchors. History service allows validators to query for older trust anchors.
DNSKEY RRsets and pick up the rollover trail where they left off.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

1. Introduction

DNSSEC [RFC4034] validators that have been offline or have missed an (emergency) rollover can use trust history service to get back on track. The trust history location is assumed available from the validator configuration. The validator then fetches old DNSKEY RRsets and checks they form a chain to the latest key.

Providers of trust history can fetch the DNSKEY data as published by the zone they track, and copy-and-paste it. They need not sign nor hold private keys safe. The algorithms for this are explained below.

2. Trust History Lookup

The algorithm is in steps. The TALINK RR type is defined below.

Step 1. The validator performs a DNSKEY lookup to the target zone, which looks like any other initial DNSKEY lookup for a trust anchor. If the keyset verifies with the trust anchor currently held, the keyset already works. Otherwise, store this result, the further algorithm either ends with this result or fails.

Step 2. Fetch the trust history list end points. Query type TALINK to the location configured for trust history.

Step 3. Go backwards through the trust history list. Verify that the keyset validly signs the next keyset. This is [RFC4034] validation, but the RRSIG expiration date is ignored. Replace the owner domain name with the target zone name for verification. One of the keys that signs the next keyset MUST have the SEP bit set. Query type TALINK to get previous and next locations. If all SEP keys have the REVOKE flag set at this step, and the keyset is signed by all SEP keys, then continue but store that the end result is that the trust point is deleted, see Section 5 [RFC5011].

Step 4. When the trust anchor currently held by the validator verifies the keyset, the algorithm is done. The validator SHOULD store the result on stable storage. Use the new trust anchor for validation (if using [RFC5011], put it in state VALID).
3. Trust History Tracker

   The tracker polls the target zone DNSKEY RRset regularly. Ignore
date changes in the RRSIG. Ignore changes to keys with no SEP flag.

   Copy the newly polled DNSKEY RRset and RRSIGs, change the owner name
to a new name at the history location. Publish the new RRset and
TALINK records to make it the last element in the list.

   The list is stored as the DNS Resource Record type TALINK (decimal
TBD). The rdata consists of two domain names. The first name is the
start, or previous name, and the other name the end or next name in
the list. The root label ‘.’ is used at the endpoints of the list.

   The presentation format is the two domain names. The wire encoding
is the two domain names, with no compression so the type can be
treated according to [RFC3597]. The list is a double linked list,
because this empowers low memory hosts to perform consistency checks.

4. Example

   In this example tuhi.example.com provides trust history for
example.net. The DNSKEY rdata and RRSIG rdata is omitted for
brevity, it is a copy and paste of the data from example.net.

   $ORIGIN tuhi.example.com.
   @ TALINK h0.tuhi.example.com. h2.tuhi.example.com.

   h0 TALINK . h1.tuhi.example.com.
   h0 DNSKEY ...
   h0 RRSIG ...

   h1 TALINK h0.tuhi.example.com. h2.tuhi.example.com.
   h1 DNSKEY ...
   h1 RRSIG ...

   h2 TALINK h1.tuhi.example.com. .
   h2 DNSKEY ...
   h2 RRSIG ...

5. Security Considerations

   The trust history tracker only provides a cached copy of old data.
The history data can be altered or withheld; the lookup algorithm
then fails.

   The security depends on the key that the validator is holding, and
the keys in the chain up to the present. If the old key held by the
validator is too old, the validator MAY not accept this risk, and then SHOULD perform out of band key priming.

If a validator is also using RFC5011 for the target zone, then the trust history algorithm SHOULD only be invoked if the last RFC5011 successful probe was more than 30 days ago. If a new key has been announced, invoke the history if no 2 probes succeeded during the add hold-down time and there was no successful probe after the add hold-down time passed. Therefore the time of the last successful probe MUST be stored on stable storage.

The algorithm looks up the initial DNSKEY like other validators do, and then walks the history in reverse. This avoids exposing the validator on the network as a host with an older key and the key id.

The SEP bit is checked to make sure that control over the KSK is necessary to change the keyset for the target zone.

6. IANA Considerations

Resource record type TALINK should refer to this RFC, it has RR type number TBD (decimal) [by dnsext expert review].

7. References

7.1. Informative References


7.2. Normative References


Author’s Address

Wouter Wijngaards
NLnet Labs
Science Park 140
Amsterdam 1098 XG
The Netherlands

Phone: +31-20-888-4551
EMail: wouter@nlnetlabs.nl