dnsop
Internet-Draft
Intended status: Standards Track
Expires: February 4, 2017

W. Hardaker
Parsons, Inc.
W. Kumari
Google

August 3, 2016

Security Considerations for RFC5011 Publishers
draft-hardaker-rfc5011-security-considerations-01

Abstract

This document describes the minimum requirements which a publisher of a zone must wait before using a new DNSKEY advertised using the RFC5011 DNSKEY rollover process.

Status of This Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on February 4, 2017.

Copyright Notice

Table of Contents

1. Introduction 2
1.1. Requirements notation 3
2. Background 3
3. Terminology 3
4. Timing associated with RFC5011 processing 3
5. Denial of Service Attack Considerations . . 3
5.1. Numerical Concrete Attack Example . . 3
5.1.1. Attack Timing Breakdown 4
6. Proper Timing Requirements 5
7. IANA Considerations 6
8. Operational Considerations 6
9. Security Considerations 6
10. Normative References 6
Appendix A. Changes / Author Notes. 6
Authors' Addresses 6

1. Introduction

RFC5011 [RFC5011] defines a mechanism by which DNSSEC validators can extend their list of trust anchors when they've seen a new key. However, RFC5011 [intentionally] provides no guidance to publishers of DNSKEYs about how long they must wait before such a new key is actually usable. Because of this lack of guidance, DNSSEC publishers may derive incorrect assumptions about safe usage of the RFC5011 process. This document describes the minimum security requirements from a publishers point of view and is intended to compliment the guidance offered in RFC5011 (which is designed to solely represent the Validating Resolvers point of view).

The authors reached out to 5 DNSSEC experts and asked them how long they must wait before using a new KSK that was being rolled according to the 5011 process. All 5 experts answered with an insecure value, and thus the authors have determined that this lack of operational guidance is causing security concerns. This document will hopefully help rectify this problem.

One important (temporary?) note about ICANN's upcoming KSK rolling plan for the root zone: the timing values, at the time of this writing, chosen for rolling the KSK in the root zone appear completely safe, and are not in any way affected by the timing

concerns introduced by this draft

1.1. Requirements notation

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 [RFC2119].

2. Background

The RFC5011 process describes a process by which a Validating Resolver may accept a newly published KSK as a trust anchor for validating future DNSSEC signed records. This document augments that information with additional constraints, as required from the DNSKEY publication point of view. Note that it does not define any other operational guidance or recommendations about the RFC5011 process from a publication point of view and restricts itself to solely the security and operational ramifications of switching to a new key too soon. Failure of a DNSKEY publisher to follow the minimum recommendations associated with this draft will result in potential denial-of-service attack opportunities against validating resolvers.

3. Terminology

foo bar

4. Timing associated with RFC5011 processing

TBD

5. Denial of Service Attack Considerations

If an attacker is able to provide a RFC5011 validating engine with past responses, such as when it is in-path or able to otherwise perform any number of cache poising attacks, she may be able to leave the RFC5011-compliant validator without an appropriate DNSKEY trust anchor.

The following timeline illustrates this situation.

5.1. Numerical Concrete Attack Example

These assumptions are used in the example scenario within this section.

TTL (all records) 1 day

DNSKEY RRSIG Signature Validity 10 days

Zone resigned every 1 day

Given these assumptions, the following sequence of events depicts how a Trust Anchor Publisher (XXX: TERM!) which waits for only the RFC5011 hold time timer length of 30 days subjects its users to a potential Denial of Service attack. The timing schedule listed below is based on a new Key Signing Key (KSK) being published at T+0, and where all numbers in this sequence refer to days before and after such an event. Thus, T-1 is the day before the introduction of the new key, and T+15 is the 15th day after the key was introduced into the zone being discussed..

In this dialog, we consider two keys being published:

K_old The older KSK being replaced.

K_new The new KSK being transitioned into active use, using the RFC5011 process.

In this dialog, the following actors are discussed:

Zone Signer The owner of a zone intending to publish a new Key-Signing-Keys (KSKs) that will become a trust anchor by validators following the RFC5011 process.

RFC5011 Validator A DNSSEC validator that is using the RFC5011 processes to track and update trust anchors.

Attacker An attacker intent on foiling the RFC5011 Validator's ability to successfully adopt the Zone Signer's K_new key as a trust anchor.

5.1.1. Attack Timing Breakdown

The following series of steps depicts the timeline in which an attack occurs that foils the publisher of a new key who revokes the old key too quickly.

T-1 The last signatures are published by the Zone Signer that signs only K_old using K_old.

T-0 The Zone Signer adds K_new to his zone and signs the zone's key set with K_old. The RFC5011 Validator retrieves the new key set and corresponding signature set and notices the publication of K_new. The RFC5011 Validator starts the hold-down timer for K_new.

T+5 The RFC5011 Validator queries for the zone's keyset per the Active Refresh schedule, discussed in Section 2.3 of RFC5011. Instead of receiving the intended published keyset, the Attacker

successfully replays the keyset and associated signatures that they recorded at T-1. Because the signature lifetime is 10 days (in this example), the replayed signature and keyset is accepted as valid (being only 6 days old) and the RFC5011 Validator cancels the hold-down timer for K_new.

T+10 The RFC5011 Validator queries for the zone's keyset and discovers K_new again, signed by K_old (the attacker is unable to replay the records at T-1, because they have now expired). It starts the hold-timer for K_new again.

... The RFC5011 Validator continues checking the zone's key set and lets the hold-down timer keep running without resetting it.

T+30 The Zone Signer believes that this is the first time at which some validators might accept K_new as a new trust anchor. The hold-down timer of our RFC5011 Validator is at 20 days.

T+35 The Zone Signer mistakenly believes that all validators following the Active Refresh schedule should have accepted K_new as a the new trust anchor (since 30 days + 1/2 the signature validity period would have passed). The hold-time timer of our

RFC5011 Validator is at 25 days and has not actually reached its 30 day requirement though.

T+36 The Zone Signer, believing K_new is safe to use, switches their active KSK to K_new and publishes a new key set signature using K_new as the signing key. Because our RFC5011 Validator still has a hold-down timer for K_new at 26 days, it will fail to validate this new key set and the zone contents will be treated as invalid.

6. Proper Timing Requirements

Given the attack description in Section 5, the correct length of time required for the Zone Signer to wait before using K_new is:

```
waitTime = addHoldDownTime
           + 3 * (DNSKEY RRSIG Signature Validity) / 2
           + 2 * MAX(TTL of all records)
```

For the parameters listed in Section 5.1, this becomes:

```
waitTime = 30 + 3 * (10) / 2 + 2 * (1)  (days)
waitTime = 47                           (days)
```


7. IANA Considerations

This document contains no IANA considerations.

8. Operational Considerations

A companion document to RFC5011 was expected to be published that describes the best operational considerations from the perspective of a zone publisher. However, the companion document was never written but the authors of this document hope that it will at some point in the future. This document is intended only to fill a single operational void that results in security ramifications (specifically a denial of service attack against an RFC5011 Validator). This document does not attempt to document any other missing operational guidance for zone publishers.

9. Security Considerations

This document, is solely about the security considerations with respect to the publisher of RFC5011 trust anchors / keys.

10. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC5011] StJohns, M., "Automated Updates of DNS Security (DNSSEC) Trust Anchors", STD 74, RFC 5011, DOI 10.17487/RFC5011, September 2007, <http://www.rfc-editor.org/info/rfc5011>.

Appendix A. Changes / Author Notes.

-00 to -01:

- Renamed Kold, Knew, we Knew it would be confusing to read.
- Added "Proper Timing Requirements" with equasion. Somehow we forgot that in original version.

Authors' Addresses

Wes Hardaker
Parsons, Inc.
P.O. Box 382
Davis, CA 95617
US

Email: ietf@hardakers.net

Warren Kumari
Google
1600 Amphitheatre Parkway
Mountain View, CA 94043
US

Email: warren@kumari.net