DNSSEC Key Management

Part 2 of 3 – Key Rollover

Agenda

- Introductions & Logistics
- Who is ISC?
- DNSSEC Key Management
- DNSSEC and ISC Services
- Wrap-up & Questions

About the presenters

- Alan Clegg
  - ISC Training and Support Engineer

    e-mail - **aclegg@isc.org**

    twitter - **@knobee**

- Larissa Shapiro
  - ISC Product Manager

    e-mail - **larissas@isc.org**

    twitter - **@ISCdotORG**

Webex Logistics

- Presentation will be about 45 minutes
- Questions may be sent to the Q&A window at any time
- Questions will all be answered at close of session
- Slides and webex audio archive will be available at

  `http://www.isc.org/webinars`

  within two days.

Who is ISC?

Internet Systems Consortium, Inc. (ISC) is a non-profit 501(c)(3) public benefit corporation dedicated to supporting the infrastructure of the universal connected self-organizing Internet—and the autonomy of its participants—by developing and maintaining core production quality software, protocols, and operations.

BIND 10

The next big thing in DNS and DHCP

Open Source Software

Quality Network Protocol Capabilities for Everyone

ISC Professional Services

Support Development
Training Consulting
Audit Design

Call in the experts!

Hosted@

Public Benefit Hosting for the Common Good

Public Benefit

Expanding the Internet through rough consensus, running code, and Open Source

DNSSEC

.com is signed, are you ready?

Get it Done!

IPv6

It works, It's live, you're going to need it.

Call the experts to help make it happen.

SIE

Changing how the security communities productively collaborate

And now our feature presentation....

DNSSEC from 30,000 feet

- DNSSEC relies on signatures to prove validity of DNS data
- Keys create the signatures
- We create (and maintain) the keys

Key Rollover

- Keys have no “expiration” dates
- If the keys never expire, why change them?
  - The longer keying material is “visible”, the more likely it is to be compromised
  - Private keying material may be stolen
  - Algorithms may be discovered to be weak

Key Rollover

- The magic of key rollover is to never allow any validating resolver to lose visibility to signatures for which it also has a key – while changing from one key to another

- TTLs make this trickier than you may expect .. but not hard if you plan ahead.

Key Rollover

- Key Signing Key and Zone Signing Keys serve different purposes
  - ZSKs sign authoritative zone data
  - KSKs sign DNSKEY resource record only
- Many more ZSK created signatures exist than KSK created ones

How to roll a key

- There are a number of ways to roll a key...
- Two of them are covered here:
  - Double Signing
  - Key Pre-Publication

Double Signing Rollover

- Used primarily for KSK rollover
  - The only record signed with KSK is the `DNSKEY` record
  - Doubling signature won't bloat zone
  - Can't replace the KSK without changing `DS` record in parent zone

Double Signing Rollover

- Simplest key rollover procedure:
  - New key is created and inserted into zone
  - All records signed with new key are signed twice
  - After records (with new signatures) are available everywhere, remove old key and signatures

Key Signing Key rollover

1. Generate new KSK
2. Insert new key into zone's `DNSKEY` RRset and use both keys for signing
3. Send new `DS` record(s) to the parent
4. Wait until the `DS` is introduced and propagated and then for the TTL of the old `DS` to pass
5. Remove the old key & re-sign

Pre-Publication Rollover

- When adding an extra signature to every authoritative resource record in your zone just doesn't work...

- Consider pre-publishing the key instead

Pre-Publication Rollover

- Pre-publication entails creating and inserting the new key without using it for signing purposes

- When all validating recursive servers have had time to expire the old `DNSKEY` resource record set, sign with only new key

Pre-Publication Rollover

- Remote servers will still need the old key to remain available until all signatures created with it have expired

- Length of time for maintaining the old key is determined by the longest TTL in the signed zone

Pre-Publication Rollover

- Since the only change to the zone is the introduction (but not use) of the new key, the only change in size of the zone is the added `DNSKEY` record

- The zone doesn't bloat up like double signing, but keeping the key around does complicate timing

Zone Signing Key rollover

1. Generate new ZSK
2. Publish both keys, but use only the old one for signing
3. Wait at least propagation time and then the TTL of the `DNSKEY` RR
4. Use new key for zone signing, leaving the old one published
5. Wait for propagation and then the maximum TTL in the old zone
6. Remove old key & re-sign

Automation of Keying

- BIND 9.7 (DNSSEC for Humans) introduced date meta-data into keys:

Publication	Default: Now
Activation	Now
Revocation (RFC-5011)	None
Inactivation	None
Deletion	None

Automation of Keying

- When generating, these dates may be provided on the command line to '`dnssec-keygen`'
- Dates can be manipulated using the new '`dnssec-settime`' command
- Dates are used by `named` automatically if so configured

Timing Meta-Data

- To pre-publish a KSK without signing:

```
dnssec-keygen -K keydir \
  -f ksk -A none example.com
[...]Kexample.com.+005+11353

rndc loadkeys example.com
```

Timing Meta-Data

- Once you are ready to sign the zone with the given key:

```
dnssec-settime -K keydir \
  -A now Kexample.com.+005+11353
rndc loadkeys example.com
```

Timing Meta-Data

- To no-longer sign with the key, but leave it in the zone:

```
dnssec-settime -K keydir \
  -I now Kexample.com.+005+11353
rndc loadkeys example.com
```

Timing Meta-Data

- And finally, remove the key from the zone:

```
dnssec-settime -K keydir \
  -D now Kexample.com.+005+11353
rndc loadkeys example.com
```

Or, if you know when...

```
dnssec-keygen -P now -A now+30d
    -I now+2y -D now+25mo
    example.com
rndc loadkeys example.com
```

- Insert into `DNSKEY` RRset now, use for signing in 30 days, retire in 2 years, delete in 2 years 1 month...

Key Rollover Consideration

- "Cracking" a key can be aided by the availability of plain-text and the associated signatures

- The more often you roll you Zone Signing Key, the more often you produce new plain-text (the `DNSKEY` RRSet) and the signatures associated with it...

Key Rollover Consideration

- Simplistic Conclusion:

  If you roll ZSK often, you weaken your KSK!

  Leading to the need to roll your KSK more often... (ugh!)

References

- DNSSEC Operational Practices

  RFC 4641

- DNSSEC Key Timing Considerations

  `draft-ietf-dnsop-dnssec-key-timing-02`

- Automated Updates of DNS Security (DNSSEC) Trust Anchors

  RFC 5011

DNSSEC Services at ISC

- BIND Forum
- Software Support
- Consulting and Custom Development
- Training

Training Schedule

- 3-Day IPv6 Fundamentals Workshop, June 7-9 Redwood City, CA
- 3-Day IPv6 Fundamentals Workshop, June 6-8 Amsterdam, NL
- 2-Day ISC DHCP Workshop, June 9-10 Amsterdam, NL
- 5-Day Intro & Advanced DNS & BIND, July 11-15 Redwood City, CA
- 5-Day Intro & Advanced DNS & BIND, Topics, Aug 1-5 Chicago, IL
- 3-Day DNSSEC Workshop, Aug 17-19 Washington, DC
- 3-Day IPv6 Fundamentals Workshop, Aug 22-24 Washington, DC
- 5-Day Intro & Advanced DNS & BIND Topics, Oct 24-28, Michigan
- 5-Day Intro & Advanced DNS & BIND, Nov 14-18 Atlanta, GA
- 3-Day DNSSEC Implementation, Nov 15-17 Rome, Italy
- 3-Day IPv6 Fundamentals, Nov 21-23 Cape Town, South Africa
- 2-Day ISC DHCP Workshop, Nov 24-25 Cape Town, South Africa
- 3-Day DNSSEC Implementation, Nov 30-Dec 2 Los Angeles, CA
- 3-Day IPv6 Fundamentals Workshop, Dec 5-7 Los Angeles, CA

Save on DNSSEC Training..

- Attendees of this call will get:

10% discount on any Public 3-day *DNSSEC* or *5-day Intro & Advanced with DNSSEC* course.

Good for 90 days, any training this calendar year, but you must register within 30 days.

Coupon code will be in the follow up email.

Upcoming Webinars

- Summer webinars will include sessions on Anycast, the new ISC Knowledge Base, and the Domain Survey. Tell us what topics you are interested in!

- Schedule and more information soon at http://www.isc.org/webinars

Questions or comments?

Thanks for attending.

isc.org