DNSSEC Validator DHCP Options

draft-mglt-homenet-dnssec-validator-dhc-options-02.txt

D. Migault

07/11/2013- IETF88- Vancouver

Table of Contents

- Problem Statement
- Time DHCP Option
- KSK DHCP Option

Problem Statement

We want our end users to use DNSSEC in their Home Networks

- Our target was primarily CPEs that are on shelves
- But we think it can be generalize to any device
- The architecture MUST be designed for DNSSEC-only resolutions.

The problem is that DNSSEC cannot be performed when:

- Time shift is too much important
- When the KSK considered for signature check is not valid/unknown

Problem Statement

We are looking for:

- Providing correct Time to the resolver
- Making sure the DNSSEC validator has not a deprecated KSK
  - 1) Provide the KSK
  - 2) Inform the DNSSEC validator these KSKs have been reported to have performed a bad key roll over.
    - Flush them if they are in your cache
    - and .... <- specify what SHOULD be done.

Problem Statement: Clarification

When does it happen?

- Devices have time derivation
- Devices do not store time
- CPE are on shelves while the Root KSK performs a key roll-over
- An emergency key roll over occurs for any KSK
- With split DNS the private zone may not have a public KSK

However, in a perfect World:

- KSK roll over do not cause any problems
- Only Root KSK procedure should be considered

Problem Statement

Questions: Do we agree that:

- Bad KSK/time results does not make DNSSEC validation possible?
- It is a problem that we must address and document.

Problem Statement: What we do not want

- Doing DNSSEC, and DNS in case of failure do DNS
  - This is DNS
- Doing DNSSEC except for case 1, 2, ..., 167980
  - This brings complexity, bugs an security vulnerabiliies
- This will not happen
  - This is wrong
- Reboot fix the problem
  - Good way to perform DoS
- It should be fixed by the DNS guys
  - Calls on the hot line are not handled by anyone but the ISP
- Firmware update should fix that
  - We are unlikely to perform this upgrades

We considered addressing these two issues by using DHCP Options

Time DHCP Option

Why a Time Option?

- To make DNSSEC-validation from boot.

Providing IP addresses (instead of FQDN) in the Network Time Protocol (NTP) Server Option for DHCP avoids DNS(SEC) resolution.

- We rely on NTP and security mechanisms assuming:
  - There is an NTP client in the device
  - The NTP TA is less likely to have emergency key roll over as the DNS one
- Can we assume this? [YES]

KSK DHCP Option

From ML/F2F there are different scenarios to consider:

- 1) Private DNSSEC (Split-DNS):
- 2) Deprecated KSK stored in cache

1) Private DNSSEC (Split-DNS):

- You may use the same private key for private and public zone
  - Probably a bad idea (sharing / NSEC3)
- You may provide the KSK
- You are the owner of the KSK
- Protected (corporate environment) / Unprotected (LoF)

KSK DHCP Option

2) Deprecated KSK stored in cache

- You are not responsible for this KSK
- A) You MAY inform the EU the KSK has been reported as deprecated.
  - Flush from cache.
  - Get KSK from the DNS infra when published
  - Pro: still rely on the DNSSEC to get the KSK.
  - Pro: Limited impacts
  - Con: Does not work for the Root Key.

KSK DHCP Option

- B) MAY provide the new/valid KSK.
  - Flush the cache
  - Replace the KSK with the new one.
  - Pro: works with the Root Key
  - Pro: Does not rely on cache update to get the valide KSK
  - Con: Does not rely on DNSSEC and requires information to be authenticated

Remaining problem: What do we do with data previously validated with the deprecated KSK?

KSK DHCP Option

Here are our questions:

- Do you agree with these two use cases?
- Comments about KSK provisioning?

Providing KSKs

We need to find a way to provision the KSKs:

- It is done for the Root KSK
- Currently, it cannot be generalized for other KSKs (non Root)
- We hope we can provide a more standard way

Providing KSKs

The big issue in KSK provisioning is:

- Can the device trust the provisioning entity?
- Who does the device trust?

Providing KSKs

We considered three cases:

- You trust the received DHCP responses
  - DHCP messages are not compromised
  - DHCP Server providing the information is not a rog DHCP Server
  - Then, the DHCP Server can provide the KSK RRsets
  - You "should" be able to insert the KSKs in your cache/boot file.
- You do not trust the DHCP responses, but you trust a CA
  - The CA Public key is less unlikely to roll over
  - The DHCP Server can provide KSK signed by the CA
  - You "should" be able to insert the KSKs in your cache/boot file.
- You trust neither the DHCP responses nor a CA
  - DHCP Option are of no help,
  - Do not request them.

Providing KSKs

The document defines two ways to provision KSK via DHCP Options

- KSK RRset
- Certificate

Thus we also define a certifiacte format for KSKs

- keyUsage set to digitalSignature (0) and nonRepudiation (1).
- Subject Alternative Name DNS name indicates the name of the zone.
- Extended usage?

Thank you for your attention