SSAC Advisory and Comments on DNSSEC Key Rollover in the Root Zone

Russ Mundy

SAC063: SSAC Advisory on DNSSEC Key Rollover in the Root Zone

Overview

- This SSAC published an advisory in November 2013 on issues relating to the rollover of the Domain Name System Security Extensions (DNSSEC) Key-Signing Key (KSK).

- The Advisory explores the following topics:

  - Terminology and definitions relating to DNSSEC key rollover in the root zone;

  - Key management in the root zone;

  - Motivations for root zone KSK rollover;

  - Risks associated with root zone KSK rollover;

  - Available mechanisms for root zone KSK rollover;

  - Quantifying the risk of failed trust anchor update; and

  - DNS response size considerations.

Recommendations

Recommendation 1: Internet Corporation for Assigned Names and Numbers (ICANN) staff, in coordination with the other Root Zone Management Partners (United States Department of Commerce, National Telecommunications and Information Administration (NTIA), and Verisign), should immediately undertake a significant, worldwide communications effort to publicize the root zone KSK rollover motivation and process as widely as possible.

Recommendations, Cont.

Recommendation 2: ICANN staff should lead, coordinate, or otherwise encourage the creation of a collaborative, representative testbed for the purpose of analyzing behaviors of various validating resolver implementations, their versions, and their network environments (e.g., middle boxes) that may affect or be affected by a root KSK rollover, such that potential problem areas can be identified, communicated, and addressed.

Recommendation 3: ICANN staff should lead, coordinate, or otherwise encourage the creation of clear and objective metrics for acceptable levels of "breakage" resulting from a key rollover.

Recommendations, Cont.

Recommendation 4: ICANN staff should lead, coordinate, or otherwise encourage the development of rollback procedures to be executed when a rollover has affected operational stability beyond a reasonable boundary.

Recommendation 5: ICANN staff should lead, coordinate, or otherwise encourage the collection of as much information as possible about the impact of a KSK rollover to provide input to planning for future rollovers.

SAC073: SSAC Comments on ICANN Root Zone Key Signing Key Rollover Plan

Overview

- The SSAC published its comments in October 2015.
- Thanked the KSK Rollover Plan Design Team
- Noted that the SSAC published an advisory on this issue (SAC 063).
- Noted that in SAC 063, the SSAC discussed:
  - Key management in the root zone;
  - Motivations for root zone KSK rollover;
  - Risks associated with root zone KSK rollover, available mechanisms for root zone KSK rollover;
  - Quantifying the risk of failed trust anchor update, and DNS response size considerations.

Overview

- The SSAC also noted that:
  - SAC 063 contained five recommendations for ICANN and the root zone management partners.
  - There is not a comprehensive correlation of the recommendations in SAC63 with material presented in the ICANN KSK Rollover Plan.
- Asked the design team to respond directly in its final report to each of the recommendations in SAC 063, and provide rationale if it chooses not to address the SSAC recommendations.

Thank you