.br DNSSEC Algorithm Rollover

Frederico A. C. Neves
<fneves@registro.br>
GTER45 - Florianópolis - 20180522

DNSSEC no .br em um slide

- 2007-05-04 .br assinado
  - Usando RSASHA1 1024 bits
- 2009-01-15 .[com|org].br assinados
  - Com o advento do nsec3/opt-out, todas a zonas do .br assinadas
- 2010-05-31 primeira troca da KSK
  - Usando RSASHA1 1280 bits
  - Novo modelo de cerimonia usando HSMs
- 2010-06-23 DS .br aparece na raiz
- 2015-06-18 segunda troca da KSK
  - Usando RSASHA1 1536 bits
- 2018-05-21 Atualmente com 3.97M delegações, 1.05M assinadas, 26%

Motivação

- Estar preparado para uma troca de algoritmo
  - Exercitar em condições normais para uma possível emergência
  - Atual sistema de provisionamento não possui esta capacidade
- Ainda estamos usando RSASHA1
  - Já trocamos a KSK duas vezes aumentando o tamanho da chave 2010/2015
  - Apesar de não existir indícios práticos em relação a resistência do SHA1 a ataques de segunda pré-imagem, em especial em um ambiente tão restrito como DNS RDATA, já passa da hora de nos afastarmos do SHA1 – RFC 4270 Nov/2005
  - Respostas substancialmente menores (ECDSAP256SHA256)
  - Reduzir o número de chaves gerenciadas uma vez que este algoritmo já suporta NSEC3
- Sistema de provisionamento DNS escrito em 2004
  - Usa um dialeto C++ velho
  - Usa uma biblioteca DNS proprietária
  - Apresenta deficiências com gerenciamento de memória que impedem melhorias operacionais
- Arquitetura muito adaptada para a inclusão de DNSSEC em 2007 e das cerimônias de assinatura em 2010
- Atualmente já estamos portando o sistema de registro para um nova arquitetura e tecnologia

Abordagem para a troca do Algoritmo

Todas as implementações de código livre que nós conhecemos, BIND e OpenDNSSEC, implementam a abordagem liberal como descrito na RFC 6781 4.1.4. Porém este documento recomenda a abordagem conservativa.

O histórico em listas públicas registra que os validadores que seguiam o método conservativo foram convencidos a modificar suas implementações para se comportarem de forma adequada com o método liberal.

RFC 6840, de Fev/2013, há mais de 5 anos, 5.11 esclarece a linguagem confusa da 4035 que deveria ser aplicada somente para assinadores e não para validadores.

A diferença do método “liberal”, que no fundo é uma dupla-assinatura pela KSK, para o “conservativo”, é a adição de dois passos extras. Só incluindo a nova chave e removendo a velha do KEYSET, depois de incluir/remover todos os RRSIGs com o novo/velho algoritmo.

Nós temos nosso próprio sistema de provisionamento e devido a recomendação da 6781 estávamos inclinados a seguir o método conservativo, mas após o registro de uma troca de algoritmo bem sucedida pelo .SE, decidimos por exercitar ambas abordagens antes de uma decisão final. Por sorte este exercício e a sua análise subsequente poderá consolidar a informação disponível e ajudar a melhorar as práticas operacionais.

Upgrade HSM / Cerimônia 2018-2

- Em preparação para a troca do algoritmo no últimos dias 15 e 16/Maio foram efetuadas atualizações.
  - Duas HSM foram substituídas
  - Upgrade de software nas mais antigas
  - Troca total do conjunto de credencias (smart-cards) que controlam os equipamentos
  - As duas HSMs mais antigas serão utilizadas em um novo site em Fortaleza/CE após a conclusão do rollover em Set/2018
- A cerimônia 2018-2 gerou assinaturas que cobrem o período de Ago/18 a Jan/19 e ainda utilizou a KSK atual gerada na cerimônia 2015-1 (20141208) keyid 45673

Cerimônia teste troca Algoritmo

- **18/Jun** – Cerimônia teste
  - 3 zonas públicas emulando a troca no .br por método de rollover. .br atuará como o parent (raiz)

Zone	Old Algorithm	New Algorithm	Keys	Method
ecdsa-c.br	RSASHA1	ECDSASHA256	KSK/ZSK	conservative
com.ecdsa-c.br	RSASHA1-NSEC3-SHA1	ECDSASHA256	CSK	conservative
eng.ecdsa-c.br	RSASHA1	ECDSASHA256	CSK	conservative
ecdsa-l.br	RSASHA1	ECDSASHA256	KSK/ZSK	liberal
com.ecdsa-l.br	RSASHA1-NSEC3-SHA1	ECDSASHA256	CSK	liberal
eng.ecdsa-l.br	RSASHA1	ECDSASHA256	CSK	liberal

  - Usando um HSM de testes / Mesmo script de uma cerimônia real

Cerimônia teste troca Algoritmo

- **19/Jun** – Começa Rollover (todos horários em UTC)
  - 06:00 ecdsa-c.br assinaturas com o novo algoritmo incluídas na zona
    - ecdsa-l.br assinada com os dois algoritmos
- **21/Jun** – Nova Chave
  - 06:00 Nova chave com novo algoritmo incluída no KEYSET
  - 12:00 Janela de 48h com duas possibilidades de saída em 24h para a remoção do algoritmo velho e a inclusão do novo no parent
- **22/Jun** – Chave Velha
  - 12:00 KSK com algoritmo velho removida do KEYSET
  - 18:00 assinaturas com o velho algoritmo removidas
    - ecdsa-l.br algoritmo velho removido

Monitoração do Rollover

A troca recente de algoritmo do .SE foi monitorada pelo SIDN LABS. Um excelente relatório está disponível em:

https://www.sidnlabs.nl/a/weblog/keep-m-rolling-monitoring-ses-dnssec-algorithm-rollover

Em colaboração com o SIDN LABS os nossos rollovers também serão monitorados utilizando o método proposto por eles.

Cerimônia troca Algoritmo

- **23 e 24/Jul** – NIC-NU/JD OS/Software Upgrade / HSM
  - Upgrade do XFRD/Signer/HW Backup nos dois sites NU/JD
  - Preparar o HSM1-JD para backup
  - Troca do Seria para formato Juliano de YYYYMMDD## para YYYYDDD### , em preparação para o futuro incremento na frequência de publicações DNS
  - Após uma semana as publicações DNS ocorrerão a cada 5’. Atualmente ocorrem a cada 30’

Cerimônia troca Algoritmo

- **25/Jul** – NIC-NU Rollover Ceremony
  - Começa 09:00 preparando o HSM2-NU para backup
  - Gera/Valida a nova KSK-2018 no HSM1-NU
  - Exporta HSM1-NU para o HSM2-NU e para o HSM1-JD. Backup copiado para o NIC-JD
  - Importa e valida as chaves no HSM2-NU
  - Move a cerimônia para o NIC-JD com reinício às 14:00
  - Importa e valida as chaves no HSM1-JD
  - Prepara o HSM2-JD para backup
  - Exporta HSM1-JD para o HSM2-JD
  - Importa e valida as chaves no HSM2-JD
    - Nova chave KSK-2018 neste momento após estar importada em todos HSMs e testa, é declarada como válida.
  - Executar a cerimônia 2018-3 usando o HSM2-JD
    - Parâmetros para a troca do algoritmo
      - Início no dia 20/Ago com 8 possíveis janelas semanais para término ou reversão
      - Assinaturas cobrindo o período de **20/Ago** até Jan/19

Mudanças Visíveis / Datas Importantes

- **19/Jun** – Começa Test Rollover
  - [com|eng].ecdsa-[cl].br
  - 06:00
- **22/Jun** – Fim Test Rollover
  - 18:00
- **24/Jul** - SOA Juliano
- **26/Jul** – Anúncios nas listas de operadores
- **31/Jul** - Publicação DNS a cada 5’
- **20/Ago** - Começa Rollover (cronograma prevendo método conservativo)
  - 06:00 Assinaturas da ZSK com novo algoritmo incluídas na zona
- **22/Ago** – Nova KSK incluída no KEYSET as 06:00
- **23-24/Ago** – Novo DS com a IANA – Tentativa para concluir o rollover na primeira janela
- **27/Ago**
  - 12:00 KSK com algoritmo velho removida do KEYSET
  - 18:00 Assinaturas com a ZSK velha removidas – Fim do Rollover

Obrigado!

Comentários / Perguntas?