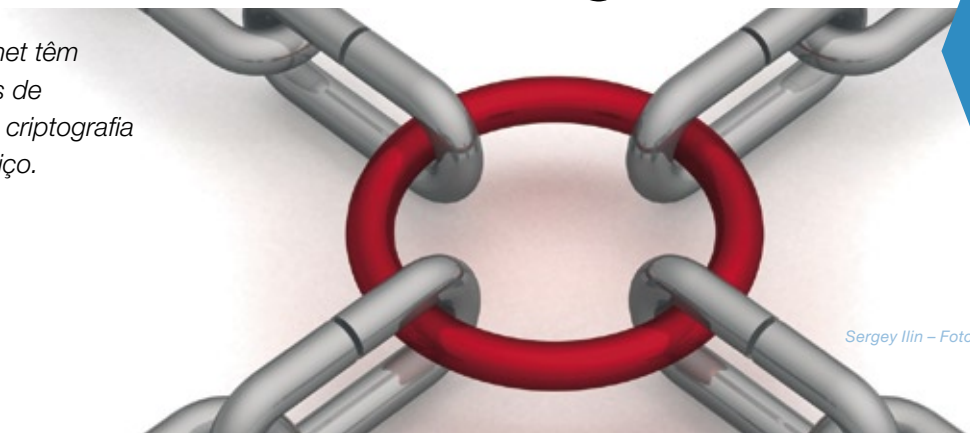
Corrente de confiança

Alguns exploits na Internet têm como alvo os servidores de nomes. O DNSSEC usa criptografia para proteger esse serviço.

por Eric Amberg



Sergey Ilin – Fotolia

Administradores de sistemas e consultores de segurança já criaram estratégias elaboradas para proteger redes de computadores, mas uma parte bem básica da infra-estrutura da Internet ainda é surpreendentemente vulnerável: o sistema de resolução de nomes. Invasores têm sofisticadas técnicas para forjar respostas DNS. É claro que os *white hats* (especialistas em segurança que agem a favor das vítimas) inventaram suas próprias manobras defensivas, mas há de se concordar que é necessária uma abordagem fundamentalmente diferente. O sistema *DNS Security Extensions* (DNSSEC)[1] oferece uma solução abrangente de autenticação e integridade de dados para o DNS.

O DNSSEC acrescenta recursos de criptografia ao serviço legado de resolução de nomes. No entanto, uma assinatura não soluciona o problema sozinha, pois o agressor também pode criar uma assinatura. O DNSSEC também necessita de um método para autenticar a chave pública usada na criptografia assimétrica, o que significa que o sistema precisa fornecer sua própria infra-estrutura de chave pública (ICP).

Reação em cadeia

Como o sistema DNS geralmente resolve nomes por meio de uma cadeia hierárquica de servidores que interagem entre si, o DNSSEC só pode garantir a autenticidade caso opere em todos os níveis da cadeia. Uma solução completa, portanto, requer a adoção do DNSSEC em grande escala. Até o momento, o domínio sueco `.se` é o único domínio de nível mais alto assinado pelo DNSSEC, mas muitas organizações já começaram a implementar e experimentá-lo em níveis mais baixos. Este artigo explicará um sistema confiável de resolução de nomes com o DNSSEC.

Chaves públicas com DNS

Em primeiro lugar, será necessário um resolvedor que suporte o DNSSEC. Como a maioria dos resolvedores genéricos não tem essa funcionalidade – e a *Libc* não é uma exceção –, os administradores de redes corporativas precisarão instalar um servidor de nomes e ativar sua funcionalidade DNSSEC.

Graças ao DNSSEC, quando os clientes nessa rede perguntarem por um IP a esse servidor, ele garantirá um retorno seguro. É claro que o salto entre o cliente e o primeiro servidor não fica resguardado, então, teoricamente, ele poderia ser manipulado. Por isso, o responsável pela segurança da rede precisa decidir individualmente se levará a sério essa falha.

O resolvedor DNSSEC então verifica se a requisição é para uma zona segurada por DNSSEC. Se o alvo solicitado estiver numa ilha segura, a resposta sempre será positiva. Os nós mais altos nessas estruturaas são chamados de *Secure Entry Points* (pontos de entrada seguros), ou SEP (**figura 1**). Os administradores devem dar prioridade máxima a essas entradas no resolvedor DNSSEC. Portanto, a lista de SEPs é o equivalente funcional ao fornecimento de um certificado por uma autoridade a um navegador web.

Ilhas solitárias

O DNSSEC usa os mesmos mecanismos de acesso que o DNS legado. Como o resolvedor solicita apenas *Resource Records* (RRs) do servidor,

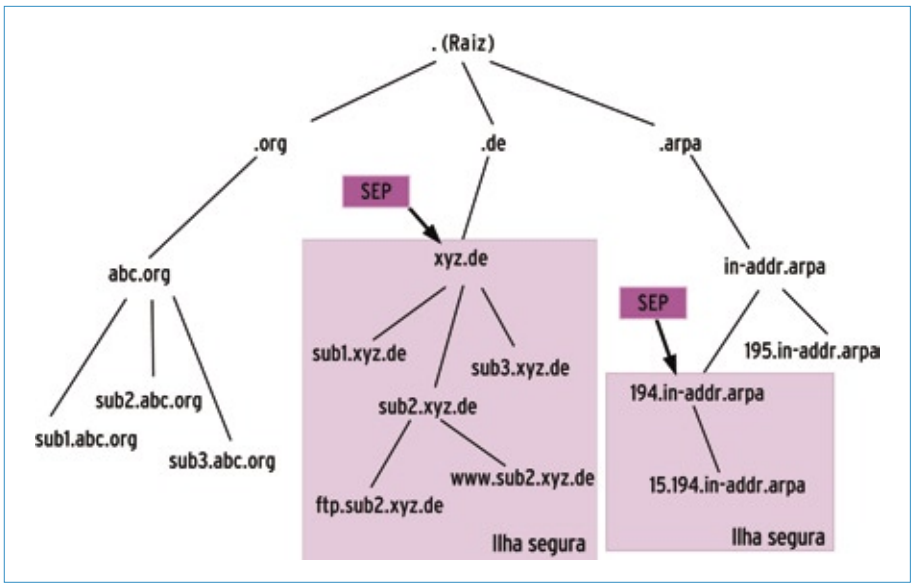


Figura 1 O *DNSSEC* adiciona SEPs à hierarquia de domínios do DNS. Depois, essas ilhas seguras vão se unir para formar um grande continente DNS.

o sistema é retrocompatível. Porém, oferece mais segurança por meio de assinaturas dos RRs. Se uma resposta não for corretamente assinada, ela será descartada.

Por jamais tentar o usuário a usar uma resposta potencialmente comprometida, essa técnica é muito segura. Porém, exige que os usuários se habituem a receber do servidor respostas *NXDOMAIN*, dizendo que o domínio não existe.

Se a resposta não vier de uma ilha segura, o resolvedor resolverá o nome pelo sistema legado. Todavia, tenha em mente que, com o DNSSEC, o usuário final não sabe se uma resposta foi ou não autenticada pelo DNSSEC.

A longo prazo, os evangelizadores do DNSSEC procuram possuir apenas um único SEP que aponte para a zona raiz do DNS. Para isso, as ilhas seguras – atualmente separadas – precisarão crescer a ponto de se encontrarem, eliminando os múltiplos SEPs de cada resolvedor DNSSEC. Até isso acontecer, será preciso definir muitos SEPs em cada resolvedor.

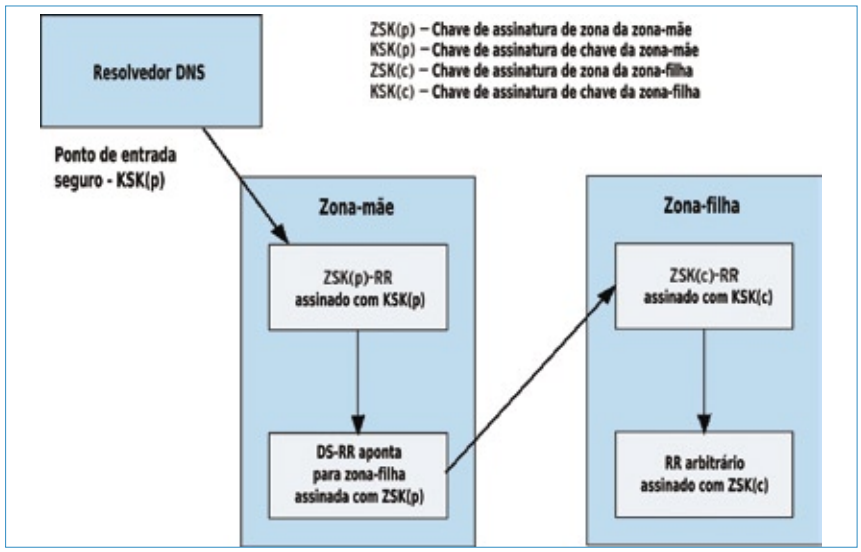


Figura 2 A KSK assina a ZSK, que assina todas as outras entradas do arquivo de zonas. O sistema ICP hierárquico segue as mesmas linhas que a estrutura do DNS.

Correntes de confiança

O DNSSEC utiliza pares de chaves assimétricas, ou seja, pares com uma chave privada e outra pública. Uma chave de assinatura de zona (ZSK) protege os RRs individuais num arquivo de zonas e, ao mesmo tempo, é protegida pela chave de assinatura de chaves (KSK) (**figura 2**).

Dentro de uma zona, basta conhecer a KSK pública para validar a ZSK e, em seguida, os RRs. Entre zonas-mãe e filha, o DNSSEC usa um RR "assinador de delegação" (DS-RR). No alto da corrente de confiança fica uma KSK, que especifica o SEP, ou *Trusted Anchor* (âncora de confiança), e designa a hierarquia de zona abaixo deste como uma ilha segura. Cabe ao administrador de cada organização adicionar esses SEPs à configuração do servidor DNSSEC.

Para fazer isso, deve-se adicionar na seção `trusted-keys` do arquivo `named.conf` as KSKs das ilhas seguras a serem suportadas (**exemplo 1**). A hierarquia deve usar as KSKs mais altas disponíveis e assegurar que as chaves tenham sido transferidas de forma confiável. Os nomes de zonas são terminados por três campos. O campo de marcadores (*flags*) define o tipo de chave; 256 significa ZSK e 257 representa KSK. O segundo valor é o campo de protocolo, que deve conter um `3`, de acordo com a RFC 4034. O terceiro valor especifica o algoritmo a usar, com `5` representando o RSA/SHA-1.

Cliente ou servidor?

O cenário padrão utiliza um servidor DNS como resolvedor na rede local para consultar um repassador na rede

do provedor. O servidor DNS valida as respostas recebidas do servidor DNS do provedor. Para conseguir fazer isso, o administrador precisa ativar, primeiramente, o DNSSEC no servidor DNS.

A opção `dnssec-enable yes;` no arquivo de configuração do *Bind*, `named.conf`, ativa a funcionalidade DNSSEC, desde que seja definida como SEP pelo menos uma chave confiável.

Assinatura de zonas

Para assinar os registros de zonas individuais, primeiro os operadores dos seus servidores DNS precisam gerar pares de chaves para seus domínios e zonas, começando pelas ZSKs e KSKs. O seguinte comando, se executado no servidor de nomes primário, cria um par de chaves para a zona *exemplo.com*:

```
# dnssec-keygen -a RSASHA1 -b \
2048 -n ZONE exemplo.com
```

A opção `-a` acima especifica os algoritmos RSA e SHA1. Embora os desenvolvedores costumem recomendar RSA com SHA-1, é possível especificar outros algoritmos, como DSA ou RSA/MD5.

O parâmetro `-b 2048` especifica o comprimento da chave, e `-n` informa ao dono do registro, que, no caso de uma zona, é `ZONE`.

A chave recém-criada será nossa ZSK. Para criar uma KSK correspondente, é necessário adicionar a opção `-f KSK` ao comando. Isso resulta num arquivo chamado `Kexemplo.com.+005+18553`, que é uma concatenação de *K* (do KSK), o nome do domínio, os algoritmos de criptografia e *hash* e uma ID de chave gerada aleatoriamente, separados por caracteres de adição. Os números dos algoritmos são `1` para RSA/MD5, `3` para DSA e `5` para RSA/SHA-1.

Após gerar as chaves, o diretório atual deve conter uma chave pública (arquivo com extensão `.key`) e uma chave privada (`.private`). Com isso, a chave pública (**exemplo 2**) já pode ser adicionada ao arquivo de zonas com a diretiva `$include`, como mostra o **exemplo 3**.

Vínculo de chaves e zonas

Após completar essa etapa, a zona já pode ser assinada com uso do comando `dnssec-signzone` acompanhado pelos parâmetros adequados:

```
dnssec-signzone -o exemplo.com \
-k Kexemplo.com.+005+42209 \
exemplo.com.zone \
Kexemplo.com.005+42209
```

A opção `-k` especifica a KSK.

Em seguida, o programa ordena os registros de zonas, adiciona registros NSEC, assina RRs *DNSKEY* com uso da ZSK e da KSK, e depois usa a ZSK para assinar os outros registros. Além disso, ele cria dois novos arquivos: `dsset-exemplo.com` e `keyset-exemplo.com`, ambos com a extensão `.signed`. Os registros de zona resultantes são exibidos em detalhes no **exemplo 4** com trechos das chaves.

Um registro *RRSIG* para cada um dos registros originais de zona é assinado pela ZSK privada. O servidor publica as duas chaves públicas, a ZSK (256) e a KSK (257), no RR *DNSKEY*. Nesse ponto, os pares de chaves assinam um ao outro e a ZSK é usada para todas as outras assinaturas.

Para impedir a remoção não autorizada de um registro de zona, os RRs ordenados são interligados para formarem uma cadeia. Ironicamente, o RR *NSEC* é um dos maiores obstáculos à difusão da cobertura pelo DNSSEC. Alguns críticos alegam que isso leva a problemas de proteção de dados, pois os agressores poderiam simplesmente consultar a cadeia para descobrir todos os registros de uma zona, que se conhece como "zone walking".

Depois de recarregar os arquivos de zonas, o servidor retorna as respostas DNS com suas próprias assinaturas. Essas assinaturas têm validade padrão de 30 dias, mas a opção `-e AAAAMMDDHHMMSS` permite modificar esse período. Se esse parâmetro for alterado, é necessário assinar a zona manualmente, mais uma vez, com o `dnssec-signzone` e as opções necessárias. Caso alguma entrada seja adicionada ou removida de uma zona, será necessário assiná-la novamente.

Depois de gravar a zona-mãe, é possível estabelecer uma corrente de confiança para estender a proteção às zonas-filhas. Um resolvedor

Exemplo 1: Configuração de DNS para SEPs

```
01 trusted-keys{
02   "exemplo.com." 257  3  5
03    "AwEAAcDKu5Kqbk92caGeQ2GjQDucJ2t6jfUb
04     gdye+zyw6qS9PorViM5ViTifFt1JYgB5RnGf
   ...
11     iv+CkVUfKbcdqpoBThBWH67VqD8kljLRsEGt
12     wRWZbGfjhuGkm56MHZCfYTk=";
13
14   "tux.local." 257  3  5
15    "AwEAAa+z+JB9qd6Q9Kg7isg/DqJdqX9Kqxpu
16     One4zGlUWNJXAT5ivVva5N4l1YOPfq2M+dJH
   ...
23     PaHbJ1vzg+G5mLFI1vEt5FTGVXWJpOGWD6yK
24     uLdrYlLOoOapQ8FG9AqMrvk=";
25 };
```

Exemplo 2: Entrada de chave para arquivo de zonas

```
01 cat Kexemplo.net.+005+18553.key
02   exemplo.net. IN DNSKEY 256 3 5 (
03     ZUPI4+OM1VO+SQmFzHQtZMuzLH3UxWEOGmG5Gfj...
04     ijandHGG8lD3IO1azWN6DiVFEVzgrOotAdDonfY...
05     =oElkw== )
```

pode usar um DS-RR para se referir a uma zona delegada. Um valor de hash nesse registro assina a KSK na zona-filha.

Ganhando confiança

O comando `dnssec-signzone` faz a assinatura e cria dois arquivos: `dsset-exemplo.com` e `keyset-exemplo.com`. O administrador da zona subordinada precisa enviar pelo menos um dos dois para o administrador da zona-mãe. O DS especificado em `dsset-exemplo.com` já contém um DS-RR correspondente para o arquivo de zonas da zona-mãe.

Depois que o administrador executa `dnssec-signzone` para a filha `sub1.exemplo.com`, uma linha como a seguinte é acrescentada ao arquivo:

```
sub1.exemplo.com. IN DS 18890 1 \
1 AE9882AD0F80C91663A1ADE3742B2F24
➥03A7283
```

Diferentemente dessa, a chave especificada no arquivo `keyset-sub1.exemplo.com` possui o registro do arquivo da zona `DNSKEY` para a zona-filha da KSK.

Isso significa que o administrador da zona-mãe pode configurar o registro `DS` armazenando a chave num arquivo com um prefixo `keyset-child`; no nosso caso, seria `keyset-child-sub1.exemplo.com`.

Todos os arquivos são guardados no diretório de arquivos de zonas. Assim que os novos arquivos estiverem em seus devidos locais, o provedor precisa assinar novamente a zona-mãe para habilitar os links. Adicionar a opção `-d` faz com que o `dnssec-signzone` crie o registro `DS` correspondente. Como alternativa, pode-se fazer um `$include` do DS especificado e assinar o arquivo de zonas da zona-mãe.

Uma vez que o registro `DS` tenha assinado a KSK na zona-filha `sub1.exemplo.com`, e supondo que um resolvedor com suporte a DNSSEC possua a KSK como uma SEP, o resolvedor então vai validar tanto a zona-mãe quanto a filha. Essa validação pode ser feita para qualquer outra zona subordinada.

Se a zona-mãe não for segura, é possível validar sua própria KSK por meio do registro *DNSSEC Lookaside Validation* (DLV). A ISC possui um registro DLV[2]. Os administradores que desejarem enviar a KSK de suas zonas para o registro DLV deverão usar a opção `-l` e especificar um endereço:

```
dnssec-signzone -l dlv.isc.org -o
➥exemplo.com -k Kexemplo.
➥com.+005+42209 exemplo.com.zone
➥Kexemplo.net.+005+18553
```

Esse comando grava o arquivo `dlvset-exemplo.com` , que deve ser enviado por email para `dlv-registry@isc.org` juntamente com o nome de domínio e o nome do administrador.

Após o registrador do DLV verificar a entrada, é criado um registro `DS` que aponta para a zona `exemplo.com`. Isso significa que o servidor de nomes da ISC é um bom SEP a ser usado publicamente.

Exemplo 3: Arquivo de zonas antes da assinatura

```
01 ; exemplo.com zone
02 ;
03 $TTL 10
04 $ORIGIN exemplo.com.
05
06 @    100 IN SOA ns1.exemplo.com. (
07        admin.exemplo.com.
08        2007112001
09        100
10        200
11        604800
12        100
13      )
14
15        NS            ns.exemplo.com.
16 ns1.exemplo.com.  A  172.16.5.1
17 a                 A  192.168.0.1
18 b                 A  192.168.0.2
19
20 $include Kexemplo.com.+005+18553.key ; ZSK
21 $include Kexemplo.com.+005+42209.key ; KSK
```

Ser ou não ser

A difusão do DNSSEC esbarra no fato de que os sistemas dos clientes (usuários finais) não costumam suportar o protocolo. Eles tendem a depender de servidores DNS locais com essa funcionalidade, e isso não deve mudar no futuro próximo.

Segurança extra

É claro que o DNSSEC não é capaz de substituir outras medidas de segurança, como VPNs e infra-estruturas de chave pública. As ICPs públicas gerenciam certificados assinados por CAs reconhecidas. E se o uso de SSL/TLS for baseado nessa tecnologia, o nível de autenticidade e confiança é bem maior do que o DNSSEC oferece.

Pontos fortes e fracos

Estabelecer uma corrente de confiança com o DNSSEC é razoavelmente fácil, mas gerenciá-la é mais difícil. Todos os envolvidos – desde a raiz até a última zona delegada por ela – precisam de chaves regularmente atualizadas para o resolvedor funcionar corretamente.

Os registros `NSEC` possibilitam a leitura de todos os registros numa zona com técnicas de *zone walking*. Como os desenvolvedores do DNS criaram o protocolo para ser aberto e livremente acessível, eles deliberadamente não projetaram o DNSSEC para confidencialidade.

Exemplo 4: Arquivo de zonas assinado

```
; File written on Wed Nov 20 17:02:12 2007
     ; dnssec\_signzone version 9.4.1
     exemplo.com.  100  IN SOA   ns.exemplo.com.  admin.exemplo.com. (
                    2007112001 ; serial
                    100        ; refresh (1 minute 40 seconds)
                    200        ; retry (3 minutes 20 seconds)
                    604800     ; expire (1 week)
                    100        ; minimum (1 minute 40 seconds)
                    )
           100 RRSIG SOA 5 2 100 20070429180412 (
                    20070330180412 17000 exemplo.com.
                    Q7QT/Y3MhD9Zx6/...= )
           100 NS     ns.exemplo.com.
           100 RRSIG NS 5 2 100 20070429180412 (
                    20070330180412 17000 exemplo.com.
                    k4Dy4YRfMwTUsKt...= )
           100 NSEC   a.exemplo.com. NS SOA RRSIG NSEC DNSKEY
           100 RRSIG  NSEC 5 2 100 20070429180412 (
                    20070330180412 17000 exemplo.com.
                    fEnDtTdDyYrC7Dq...= )
           100 DNSKEY  256 3 5 (
                    AQPI4+OM1VO55RS...=
                    ) ; key id = 18553
           100 DNSKEY  257 3 5 (
                    AQOzgs4qea+ImJ1...
                    ) ; key id = 42209
           100 RRSIG   DNSKEY 5 2 100 20070429180412 (
                    20070330180412 17000 exemplo.com.
                    hFcUzcQnsQbiOhn...= )
           100 RRSIG   DNSKEY 5 2 100 20070429180412 (
                    20070330180412 49656 exemplo.com.
                    oyum/nlrNZ7Xdxi...= )
     a.exemplo.net. 100 IN A 192.168.0.1
           100 RRSIG   A 5 3 100 20070429180412 (
                    20070330180412 17000 exemplo.com.
                    oN1QemG7B47dWBo...= )
           100 NSEC    b.exemplo.net. A RRSIG NSEC
           100 RRSIG   NSEC 5 4 100 20070429180412 (
                    20070330180412 17000 exemplo.com.
                    Kon6z25uqnHpGc9...= )
     b.exemplo.net. 100 IN A 192.168.0.2
           100 RRSIG   A 5 3 100 20070429180412 (
                    20070330180412 17000 exemplo.com.
                    lWXfx2ebTpOBvCx...= )
```

Por outro lado, confidencialidade é um objetivo inequívoco da proteção de dados.

Muitos registradores vêem o zone walking como um problema de proteção de dados. O rascunho do NSEC3 detalha uma solução potencial para esse problema, baseada em criptografia. Os céticos questionam se nomes DNS publicamente resolvíveis devem ser protegidos; apesar de enxergarem o problema de pessoas sistematicamente não autorizadas listarem as zonas, eles ressaltam que outras medidas oferecem melhores resultados na área de proteção e confiança – como ACLs e autenticação de clientes, por exemplo – mas não se estendem a registros DNS livremente disponíveis. Os especialistas dizem que outra questão que impede a introdução do DNSSEC é que seus processos criptográficos causam o dobro da carga na infraestrutura quando comparados a um servidor normal.

Conclusões

Como de costume, a política tem um papel importante no processo de adoção do DNSSEC. A questão de quem gerencia a chave privada na zona raiz ainda está em aberto. Por um lado, o RIPE e outros registradores já pediram à ICANN que assine a zona raiz o mais breve possível; por outro, algumas pessoas se preocupam com a atribuição de todo o controle de uma chave privada a uma autoridade dos EUA.

Muitos enxergam o servidor da zona raiz como a última linha de defesa contra a intervenção do Estado, e é compreensível que não se queira colocar essa zona atrás de uma chave privada. Discussões globais não impedem que administradores de zonas privadas testem e introduzam o DNSSEC. A maioria das zonas privadas não é afetada pela questão de proteção de dados do NSEC, pois contêm apenas *www*, *mail* e outros registros públicos.

Se eles publicarem uma KSK de forma central – num registro DLV, por exemplo – então terceiros poderão usar o DNSSEC sem qualquer problema.

Sempre que dados pessoais estão em jogo, assim como em bancos e compras online, os provedores podem aumentar a confiança criando uma zona protegida por DNSSEC. ■

Mais informações

[1] Documentos que especificam o DNSSEC: RFCs 4033, 4034, 4035 e 3658: http://tools.ietf.org/html

[2] Registro DLV no ISC: https://secure.isc.org/index.pl?/ops/dlv/

[3] DNSSEC na RNP: http://www.rnp.br/newsgen/9801/dnssec.html

[4] Servidor DNS ISC: http://www.isc.org/