Artigo: DNSSEC EXTENSÕES DE SEGURANÇA PARA SERVIDORES DNS

Professor Orientador: Paulo Roberto Galego Hernandes Junior
e-mail: paulo.galego@fatec.sp.gov.br

Professor responsável pela disciplina Projeto Articulador de Segurança da Informação: Sérgio Duque Castilho
e-mail professor: sergiocastilho@uol.com.br

Autora: Marli Vieira dos Santos

Graduanda em Análise de Sistemas e Tecnologia da Informação com habilitação em Tecnólogo em Segurança da Informação

FATEC – Faculdade de Tecnologia de Ourinhos

OURINHOS – SP

19/11/201

1 INTRODUÇÃO

Para acessar uma página de internet ou enviar/receber e-mails, basta que seja digitado o site no navegador, e num clique as informações solicitadas são transferidas e acessadas.

São atitudes rotineiras de usuários que apesar de parecerem simples, exigem um processo complexo, que será apresentado ao longo deste trabalho.

Sendo assim ao acessar uma página na Internet ou efetuar trocas de e-mail, a aplicação que fez a conexão inicial precisa conhecer o endereço IP da página na Internet, pois as informações serão enviadas em pacotes IP, que tem um campo de origem e destino que devem ser números IP e não "nomes" (de sites). A aplicação que faz essa requisição utiliza um sistema que associa o endereço IP a um nome, tornando o acesso à página na Internet possível através do nome dela e não do endereço IP. Este processo chama-se resolução de nomes, e é realizado por um sistema chamado *Domain Name System* (Sistema de Nomes de Domínio), ou DNS.

Quando o sistema não está funcionando, as conseqüências são graves e generalizadas. Estes problemas podem ser causados por intrusos, que se aproveitam das falhas e vulnerabilidades do sistema, que se conhecidas e exploradas, podem trazer sérias conseqüências para os serviços da Internet, tais como negação de serviço e roubo de informações.

O DNSSec, um conjunto de extensões de segurança proposto pelo IETF (Internet Engineering Task Force) para o DNS, utiliza criptografia de chaves públicas e assinaturas

digitais, disponibiliza autenticação e integridade dos dados, além de distribuição de chaves e certificação de transações e requisições.

O objetivo geral do desenvolvimento desse artigo é apresentar de forma clara o funcionamento de um dos recursos mais importantes dentro da área da internet, o DNS. Tendo como objetivo específico estudar as vulnerabilidades do serviço, demonstrar sua importância e as conseqüências que sua indisponibilidade pode provocar. Apresentar a solução DNSSEC e como ele funciona.

2 O SISTEMA DE NOMES DE DOMÍNIOS (DNS)

Um dos principais mecanismos que compõe a Internet, assim como o ar é importante para o ser humano, o DNS é para a internet. Funciona como um repositório distribuído que permite o mapeamento entre nomes de serviços e sua correspondente localização na rede.

Trata-se de um recurso usado em redes TCP/IP (o protocolo utilizado na internet e na grande maioria das redes) que permite acessar computadores pelo nome a ele associado, sem que o usuário ou sem que o próprio computador tenha conhecimento de seu endereço IP, o sistema de nomes de domínio:

> [...] é um banco de dados distribuído. Isso permite um controle local dos segmentos do banco de dados global, embora os dados em cada segmento estejam disponíveis em toda a rede através de um esquema cliente-servidor. (CAMPOS, DANTAS, 2011).

Este conjunto de grandes bancos de dados distribuídos em servidores de todo o mundo é que indicam qual IP é associado a um nome (ou seja, um endereço do tipo *www.nomedosite.com, associado a um endereço IP*), assim cada site da internet é acessível por um endereço IP. Dessa forma quando é digitado, por exemplo, IP 200.154.56.80, o endereço responderá pelo domínio correspondente www.terra.com.br. O DNS faz essa resolução de nome para IP e vice-versa.

De acordo com ALECRIM (2005), o comum é que seja digitado o nome do site e não o endereço IP, já que nomes são mais fáceis de decorar que números difíceis de IP, alem disso imagine toda vez que for acessar um site ter de procurar o número de IP ao qual o mesmo está associado, seria necessário uma grande lista.

O DNS permite o uso de nomes (também chamados de domínios) ao invés dos IPs no acesso aos sites.

Segundo o site REGISTRO.BR, o DNS possui as seguintes características: 1) Sistema Hierárquico distribuído, assim cada domínio responde as suas respectivas requisições; 2) Distribuído eficientemente, sistema descentralizado e com cachê; 3) Tradução de nomes para

números IP; 4) Não existe um repositório único de informações: conteúdo em vários bancos de dados descentralizados; 5) Informação distribuída entre milhares de computadores; 6) Estrutura em arvores, semelhante à estrutura de diretórios de sistemas Unix.

Nessa estrutura, por segurança, um domínio pode definir vários servidores DNS. Mantendo a hierarquia da estrutura, o DNS primário é o primeiro sistema a ser consultado no momento da resolução do nome, caso o servidor DNS primário esteja em manutenção, o servidor DNS secundário é consultado, e assim sucessivamente. Isso permite o intenso tráfego e a demanda de requisições executadas aos servidores, possibilitando respostas das informações, no caso os domínios esperados.

A organização responsável por atribuir nomes de domínio e endereços IP em nível global é a ICANN (Internet Corporation for Assigned Names and Numbers). Abaixo uma citação referente à estrutura hierárquica do sistema DNS:

> Devido ao intenso tráfego da internet e devido à segurança da rede, a estrutura do banco de dados DNS é distribuída e hierárquica. Ou seja, ao invés de um banco de dados central e único com informações de todos os domínios, a resolução ocorre consultando-se diversos servidores DNS e sua resolução é hierárquica (um servidor DNS pode apontar para outro servidor DNS e assim sucessivamente).
> A estrutura hierárquica equivale a uma árvore invertida, ou seja, existe um servidor principal que aponta para um secundário que aponta para um terceiro e assim sucessivamente. O servidor DNS que está no topo da internet é o servidor raiz. (*MONTEIRO, 2007)*

3 SERVIDORES NO MUNDO

Quando um computador na internet deseja acessar um domínio, ele trabalha a solicitação da direita para a esquerda. Os servidores raiz sabem quais são os servidores de topo, e estes por sua vez sabem quais são os servidores responsáveis pelo segundo nível.

"[...] Existe, atualmente, 13 servidores raiz com nome no formato letter.root-servers.net". (ZILLI, 2006, p.22).

Abaixo um mapa designando a localização dos servidores raiz espalhado pelo mundo:

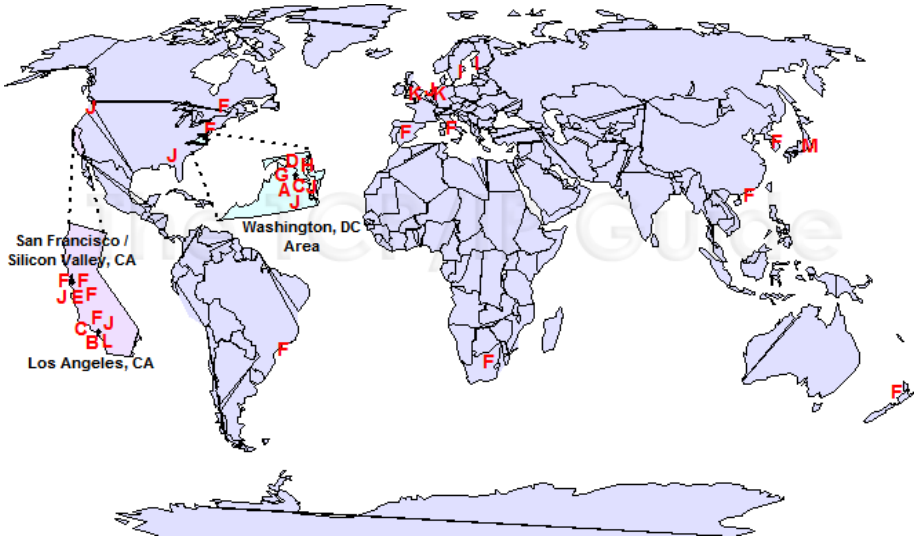

Figura 10: Mapa com DNS Raiz no mundo

FONTE: http://www.tcpipguide.com/free/t_DNSRootNameServers-3.htm

Os clones foram criados e espalhados para melhorar a velocidade de acesso. “Por segurança, o servidor raiz foi replicados em 13 servidores raízes diferentes espalhados pelo mundo e 2 vezes ao dia seu conteúdo é automaticamente replicado”. (MONTEIRO,2011).

4 PROBLEMAS E VULNERABILIDADES DO DNS

No DNS, quando uma resposta é recebida e aparentemente é quem diz ser, ou seja, parece responder a solicitação/pergunta enviada, ela é aceita como correta. Sendo assim, atacantes podem explorar essa vulnerabilidade falsificando uma resposta e fazendo com que ela chegue à origem antes da resposta legítima. O receptor vai achar que a resposta é verdadeira, aceitando-a como correta, de acordo com DAVIES, 2008. Isso pode levar os ataques de envenenamento de cachê e impersonificação do recursivo.

Este capítulo aborda as vulnerabilidades do serviço DNS, as táticas dos ataques mais comuns, abaixo uma figura para demonstrar:

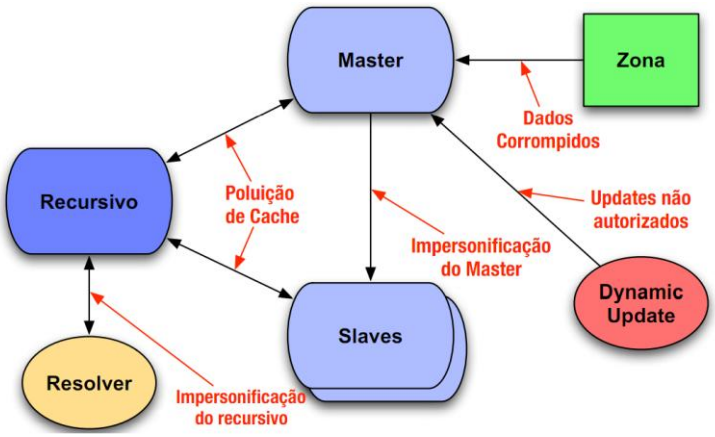

FIGURA11: ATAQUES AO SERVIDOR DNS
FONTE: ftp://200.160.2.8/pub/gts/gts12/05-PorqueDNSSEC.pdf

4.1 Impersonificação do Recursivo

Este ataque é conhecido como Man-in-The-Middle (homem no meio), ocorre quando o cliente pede ao servidor local para resolver um domínio, mas antes que o servidor DNS faca consultas recursivas para obter a solução do nome, o atacante responde mais rápido, spoofando o endereço do recursivo, abaixo uma ilustração ataque:

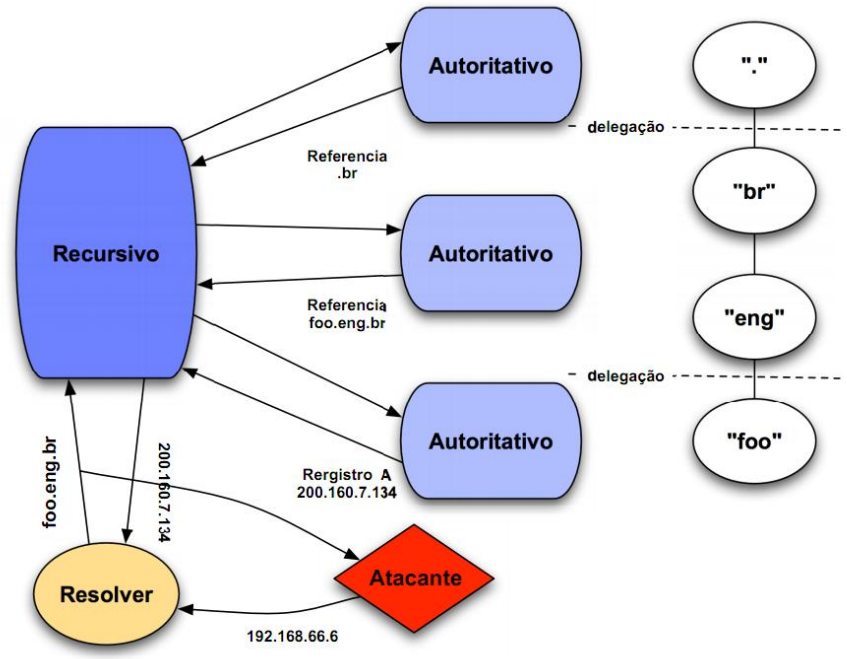

FIGURA: ATAQUE MAN-IN-THE-MIDDLE
FONTE: ftp://200.160.2.8/pub/gts/gts12/05-PorqueDNSSEC.pdf

4.2 Poluição do Cachê

Ao resolver um domínio o servidor recursivo armazena a resposta em uma memória temporária, chamada cachê, assim quando o mesmo domínio for novamente solicitado o servidor já terá a resposta armazenada, tornando dispensável consultas a outros servidores.

De acordo com DAVIES, 2008, para melhorar a eficiência, os servidores DNS tipicamente intermediaria e armazena os resultados em um cachê para acelerar pesquisas adicionais.

Porem esse mecanismo de eficiência em cachê traz consigo o risco de uma vulnerabilidade: a poluição do cachê. Quando um atacante consegue enganar um servidor, fazendo com que ele guarde em cachê uma resposta falsa, ele consegue fazer com que o servidor use essa resposta em consultas futuras. Sendo assim, com um ataque bem sucedido, o atacante consegue envenenar o cachê, o que afetará vários usuários, dessa forma quando

algum resolver solicitar este endereço novamente, as respostas continuarão a apontar para um endereço falso ate que o TTL (Time to Live) se esgote.

O Time to Live é o tempo em que uma consulta fica armazenada em cachê, ao fim deste o processo completo de consulta e executado, estando sujeito a ter o cachê envenenado novamente.

Abaixo uma ilustração do processo de ataque:

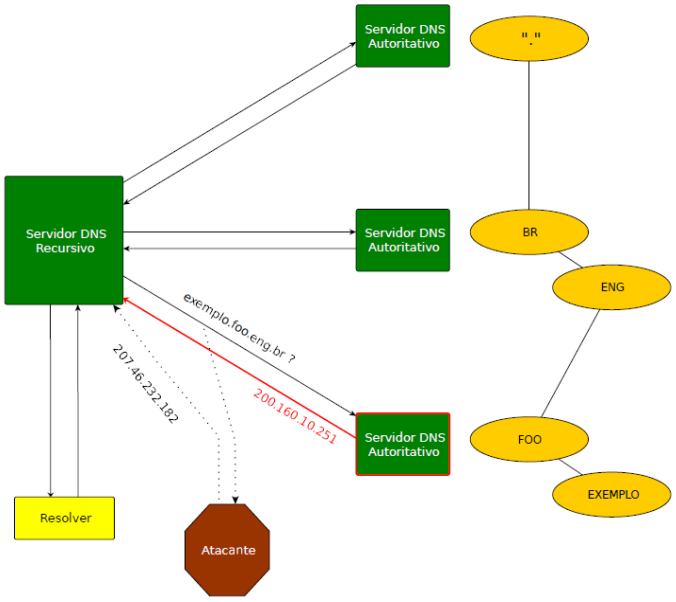

FIGURA: ATAQUE DE ENVENENAMENTO DE CACHE
FONTE: ftp://200.160.2.8/pub/doc/tutorial-dnssec.pdf

4.3 O poder dos ataques x importância da segurança

Para exemplificar o poder desses tipos de ataques, imagine, por exemplo, se durante o acesso a um site bancário sua resolução fosse feita por um servidor intruso, ou o *cache* de sua navegação estivesse envenenado, certamente, suas informações digitadas seriam interceptadas, e as conseqüências muito graves.

Abaixo uma figura representando a estatística dos incidentes reportados ao CERT.BR, no período de julho a setembro de 2011:

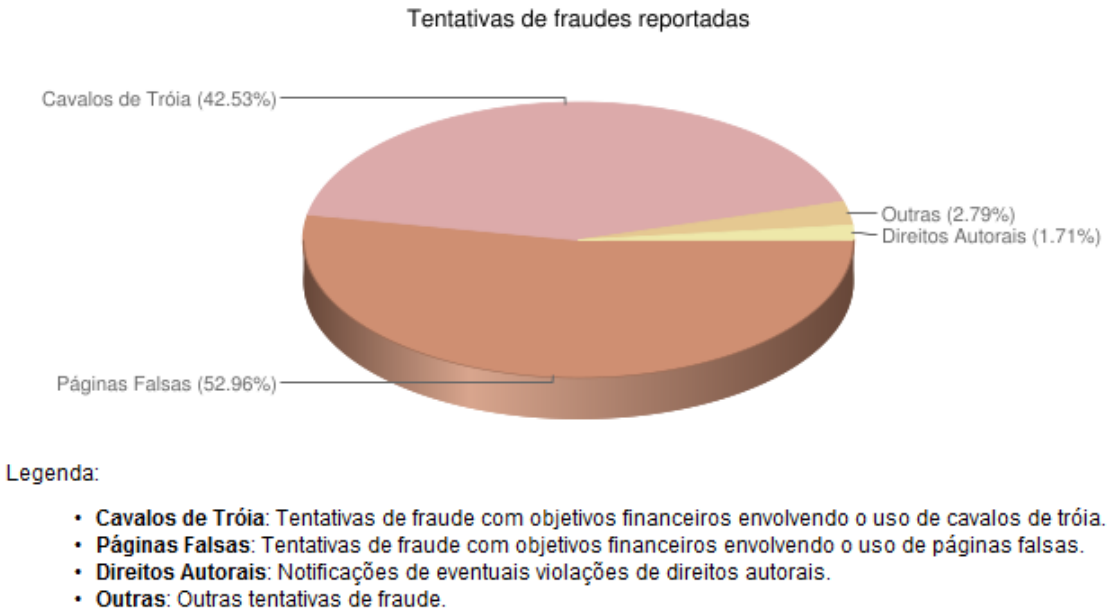

FIGURA 1: Incidentes reportados ao CERT.BR - julho a setembro de 2011

FONTE: http://www.cert.br/stats/incidentes/2011-jul-sep/fraude.html

Para exemplificar o poder desses tipos de ataques, imagine, por exemplo, se durante o acesso a um site bancário sua resolução fosse feita por um servidor intruso, ou o cachê de sua navegação estivesse envenenado, certamente, suas informações digitadas seriam interceptadas, e as conseqüências muito graves.

Albits e Liu (2001), descreverem o ataque a sevidores em 1997, no qual os usuarios que digitavam *www.internic.net* os servidores DNS com o cachê envenenados respodiam o endereço do site *www.alternic.net*.

Rohr (2009) cita um fato marcante de segurança, foi a confirmação de ataques sofisticados ao provedor de internet Virtua, que permitiram o redirecionamento do site do Bradesco e do AdSense, do Google, a endereços maliciosos, com o objetivo de roubar dados e instalar um cavalo de tróia, respectivamente.

Por esse motivo há a necessidade de transformar as operações envolvendo o DNS em um processo seguro e confiável, de maneira a diminuir ataques e simultaneamente disponibilizar mecanismos de verificação de autenticidade dos dados.

5 DNSSEC

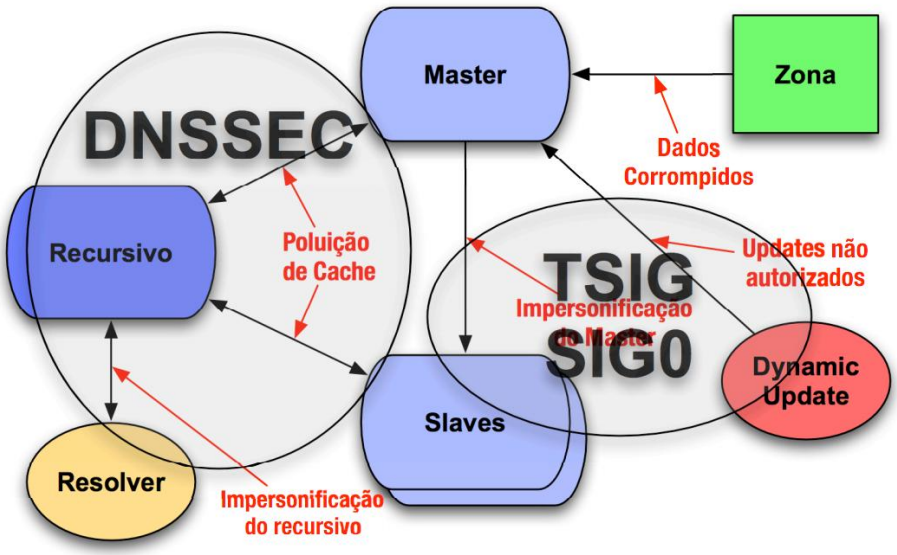

FIGURA: ATUACAO DO DNSSEC

FONTE: ftp://200.160.2.8/pub/gts/gts12/05-PorqueDNSSEC.pdf

Uma das maiores preocupações com a segurança da Internet são os servidores DNS raiz, como demonstrado no capitulo anterior, a interrupção ou invasão de um desses servidores pode gerar um caos na Internet para milhares de pessoas em todo mundo, este capitulo ira tratar da solução para os ataques apresentados anteriormente: o DNSSEC:

Assim, as alterações ao protocolo DNS foram propostas, as extensões de segurança: DNSSEC (Domain Name Security Extensions - proposto pelo IETF):

> DNSSEC é um padrão internacional que estende a tecnologia DNS. O que DNSSEC adiciona é um sistema de resolução de nomes mais seguro, reduzindo o risco de manipulação de dados e informações. O mecanismo utilizado pelo DNSSEC é baseado na tecnologia de criptografia de chaves públicas (REGISTROBR, 2011).

O serviço de DNSSec vem para manter o que existe no protocolo DNS de maneira segura, provendo autenticação e integridade dos dados. Com estes serviços, o protocolo checará se os dados publicados por uma entidade são realmente de sua autoridade (autenticidade), se os dados foram recebidos da mesma forma como foram publicados (integridade) e a garantia de que a resposta de uma consulta veio mesmo do servidor consultado, trazendo maior segurança ao usuário que estará no local (site) que realmente deseja estar.

“DNSSEC permite ao cliente não apenas para autenticar a identidade de um servidor, mas também para verificar a integridade dos dados recebidos a partir desse servidor.” (NEMETH,2000, p. 21).

Dessa forma no acesso a um site de instituição bancária o usuário saberá que as respostas do servidor são íntegras, ou seja, verdadeiras, são o que ou quem dizem ser. De acordo com a RFC 4033 estas extensões não fornecem confidencialidade.

A RFC 4035 detalha estas alterações, onde a característica principal do DNSSec, utiliza criptografia de chaves públicas e assinaturas digitais, disponibiliza autenticação da origem e proteção da integridade dos dados, além de distribuição de chaves e certificação de transações e requisições.

Quatro novos tipos de Resource Records são adicionados:

5.1 O Registro Key – Dnskey

Neste registro é armazenada a chave pública DNSKEY, DNS de chave pública, associado a um domínio.

> Nas Extensões de Segurança do DNS, ou DNSSEC, cada zona segura possui um par de chaves associado com ela. A chave privada da zona é armazenada em algum lugar seguro, geralmente em um arquivo no mesmo sistema de arquivos do servidor de nomes. A chave publica da zona é publicada como um novo tipo de registro anexado ao nome de domínio da zona, o registro KEY. (PAUL ALBITZ E CRICKET LIU, pag 375).

O DNSKEY é a chave publica enviada junto com a resposta da consulta, utilizada para validar a assinatura e garantir a integridade da consulta. O DNSKEY deve apresentar formato padrão definido, informando o protocolo e o algoritmo utilizado (ARENDS, 2005).

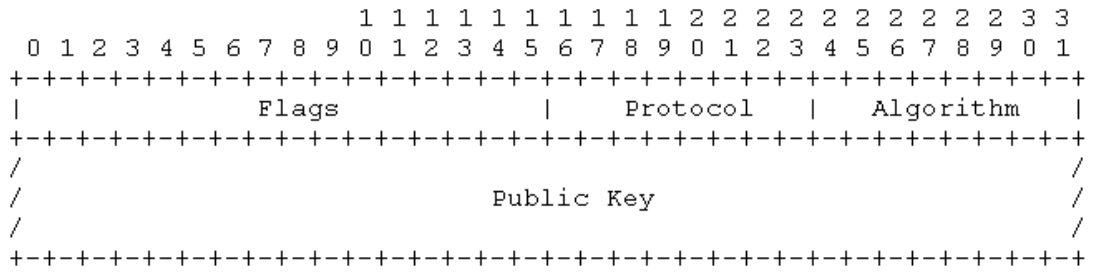

FIGURA: Formato RR DNSKEY

FINTE: http://www.rfc-archive.org/getrfc.php?rfc=4034

- O campo “Flag” deve ser um valor inteiro, para este campo os valores possíveis são: 0, 256 e 257;

- O campo “Protocol” deve ter o valor 3, se outro valor for encontrado, durante a verificação de assinatura, será considerado invalido;
- O campo “Algorithm” identifica a chave criptográfica;
- O Campo “Public Key” tem o material de chave pública, deve ser representado na base 64, formato depende do algoritmo da chave que está sendo armazenado.

Abaixo um exemplo de um DNSKEY RR que armazena uma chave para a zona example.com.

```
example.com. 86400 IN DNSKEY 256 3 5 ( AQPSKmynfzW4kyBv015MUG2DeIQ3
                                       Cbl+BBZH4b/0PY1kxkmvHjcZc8no
                                       kfzj31GajIQKY+5CptLr3buXA10h
                                       WqTkF7H6RfoRqXQeogmMHfpftf6z
                                       Mv1LyBUgia7za6ZEzOJBOztyvhjL
                                       742iU/TpPSEDhm2SNKLijfUppn1U
                                       aNvv4w==  )
```

FIGURA: Exemplo formato RR DNSKEY

FONTE: http://www.rfc-archive.org/getrfc.php?rfc=4034

- “example.com.”: especifica o nome do proprietário;
- “86400”: especifica o TTL;
- “IN DNSKEY”: especifica a classe e tipo de RR;
- “256”: indica que o bit chave Zone (bit 7), em o campo Flags tem valor 1;
- “3”: é o valor protocolo fixo;
- “5”: indica o algoritmo de chave pública.
- O restante de texto é uma codificação de Base64 da chave pública.

5.2 O Registro SIG - RRSIG Assinatura Do Resource Records (Rrsets)

Para autenticação em chaves criptográficas assimétricas, de um lado existe um proprietário da chave publica, bem como de outro lado deve existir o proprietário de assinatura da chave privada. O registro KEY armazena uma chave pública da zona, enquanto o registro SIG armazena a assinatura do REsource Records (RRsets).

De acordo com a RFC 4034 o registro SIG soh deve ser utilizado para transportar material de verificação (assinatura digital) utilizado para garantir a operação do DNS .

“O registro SIG armazena a assinatura digital da chave privada em um RRset. O RRset é um grupo de registros de recursos com o mesmo proprietário, classe e tipo”. (PAUL ALBITZ E CRICKET LIU, pag 377).

Abaixo o formato de uma RRSIG:

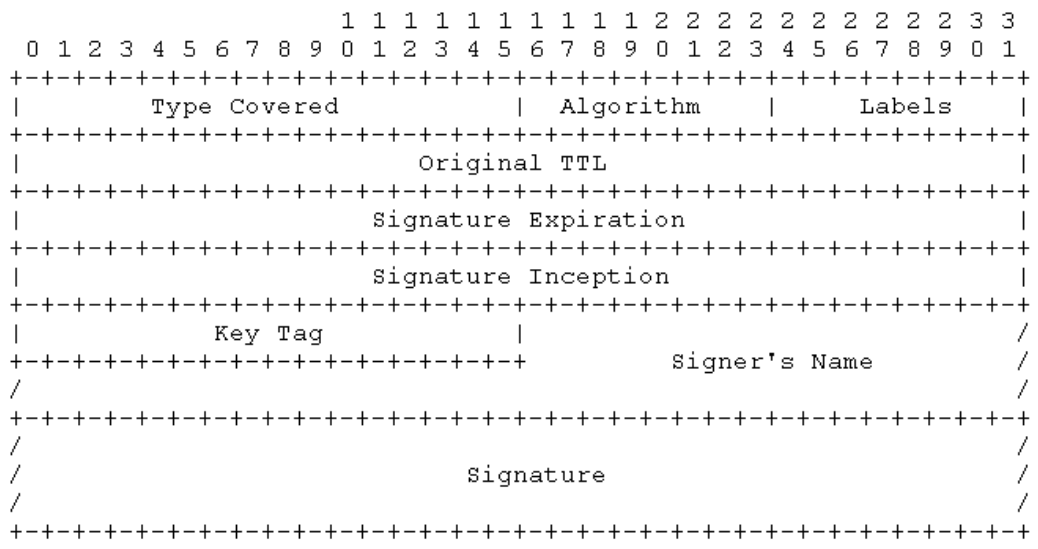

FIGURA: Formato RRSIG
FONTE: http://www.rfc-archive.org/getrfc.php?rfc=4034

- O campo “Type Covered” identifica o tipo do RRset que é abrangido pelo presente registro RRSIG;
- O campo “Algorithm” identifica o algoritmo criptográfico usado para criar a assinatura;
- O campo “Labels” especifica o número de rótulos no RRSIG originais RR nome do proprietário, pode ser usado para determinar qual era o nome do proprietário utilizado na geração da assinatura;
- O Campo “Original TTL” especifica o TTL do RRset, na zona de autoridade.
- O campo “Signature Expiration” especifica a validade da assinatura. O registro RRSIG não deve ser utilizado para autenticação nem antes da data do seu início e nem após a data de validade;
- O campo “Key Tag” valida essa assinatura, na ordem de bytes da rede;
- O campo “Signer’s Name” identifica o nome do proprietário do RR DNSKEY é usado para validar essa assinatura.
- O Campo “Signature” contém a assinatura criptográfica que cobre O RDATA RRSIG.

Abaixo um exemplo de um RR RRSIG que armazena a assinatura para a RRset do host example.com:

```
host.example.com. 86400 IN RRSIG A 5 3 86400 20030322173103 (
                                20030220173103 2642 example.com.
                                oJB1W6WNGv+ldvQ3WDG0MQkg5IEhjRip8WTr
                                PYGv07h108dUKGMeDPKijVCHX3DDKdfb+v6o
                                B9wfuh3DTJXUAfI/M0zmO/zz8bW0Rznl8O3t
                                GNazPwQKkRN20XPXV6nwwfoXmJQbsLNrLfkG
                                J5D6fwFm8nN+6pBzeDQfsS3Ap3o= )
```

FIGURA: Exemplo Formato RRSIG

FONTE: http://www.rfc-archive.org/getrfc.php?rfc=4034

- “host.example.com.”: especifica o nome do proprietário;
- “86400”: especifica o TTL;
- “IN RRSIG”: especifica a classe e tipo de RR;
- “A.”: especifica o Type covered;
- “5”: indica o Algorithm;
- “3”: indica o Labele;
- “86400”: especifica o Original TTL;
- “20030322173103”: é o valor da Signature Expiration;
- “20030220173103”: é o valor da Signature Inception;
- “2642”: indica a KeyTag;
- “example.com.”: indica o Signer`s Name;
- O restante de texto é a Signature.

5.3 O Registro Nsec

Quando um cliente (por exemplo, o servidor recursivo) recebe a resposta de uma consulta com DNSSEC habilitado, ele recebe duas informações: RRSet (registros consultados) + RRSIG (assinatura do RRSet). Se no processo de checagem esses dados não conferirem a resposta será negada.

> O registro NXT resolve o problema de assinar respostas negativas. Ele “estende” um intervalo entre dois nomes de domínio consecutivos em uma zona, indicando qual nome de domínio vem em seguida após um determinado nome de domínio. (PAUL ALBITZ E CRICKET LIU, pág. 379).

O registro NSEC armazena informações sobre o próximo nome na zona (em ordem canônica), que passa a ser ordenada. Cada registro mantém um apontador, através de seu NSEC, para o próximo registro; o último "aponta" para o primeiro. Assim é resolvido o problema de assinar respostas negativas. A figura abaixo ilustra o formato padrão do NSEC:

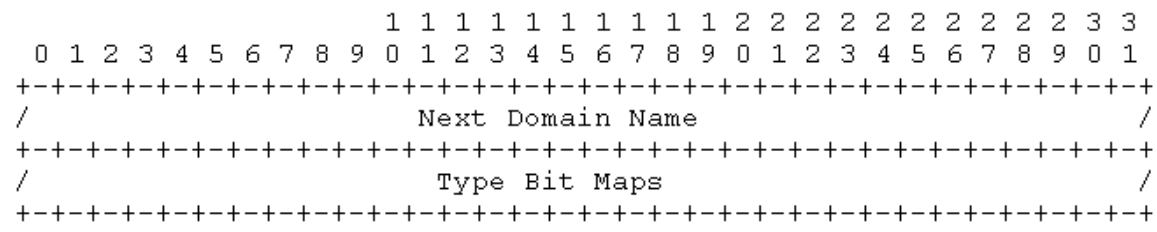

FIGURA: Formato RDATA NSEC

FONTE: http://www.rfc-archive.org/getrfc.php?rfc=4034

- O campo “Next Domain Name” contem o nome do proprietário seguinte (em ordem canônica de zona), que possui dados autorizados ou contem uma delegacao ponto NS RRset;
- O campo “Type Bit Maps” identifica os tipos RRset que existem no Nome do proprietário NSEC RR.

Abaixo um exemplo de um RR NSEC, apontando para a próximo nome oficial após o domínio alfa.example.com:

```
alfa.example.com. 86400 IN NSEC host.example.com. (
                                A MX RRSIG NSEC TYPE1234 )
```

FIGURA: Exemplo Formato NSEC

FONTE: http://www.rfc-archive.org/getrfc.php?rfc=4034

- “alfa.example.com.”: especifica o nome do proprietário;
- “86400”: especifica o TTL;
- “IN SEC”: especifica a classe e tipo de RR;
- “host.example.com”: próximo nome de autoridade em ordem canônica após o alfa.example.com;

Assim este validador poderia ser usado para provar que abc.example.com não existe. A negação autenticada de existência eh discutida em [RFC 4035].

5.4 O Registro DS Delegation Signer (Ponteiro Para A Cadeia de Confiança)

A chave pública deve ser divulgada para que os clientes possam validar as informações. A primeira solução é ter uma cópia local da chave, porém isso é ruim do ponto de vista de atualização da chave: cada cliente teria estar atento às atualizações de chave e atualizar sua cópia local com a nova versão. Isso, na prática, é muito difícil ser implementado. Outra solução seria a de utilizar algo semelhante ao processo de delegação de zonas (dados

distribuídos com "apontadores" para os próximos servidores de nomes na hierarquia) adaptado para as necessidades do DNSSEC. Daí surge o registro *Delegation Signer* (DS).

De acordo com a RFC 4034 o registro DS armazena um hash do DNSKEY da zona que será delegada. No processo de consulta recursiva, o cliente, requisita o DS da zona parent e verifica com o DNSKEY da zona que foi delegada.

O DS é um ponteiro para a cadeia de confiança, a qual garante a autenticidade das delegações de uma zona até um ponto de confiança.

Abaixo uma figura ilustrando o formato do RR DS:

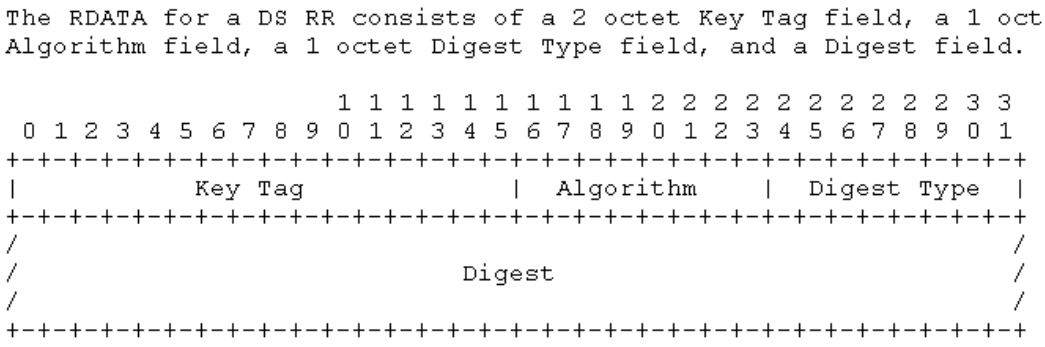

FIGURA: Formato DS

FONTE: http://www.rfc-archive.org/getrfc.php?rfc=4034

- O campo “Key Tag” lista a marca fundamental da RR DNSKEY referido pelo registro DS, na ordem de bytes da rede. A Key Tag usada pelo RR DS é idêntico a Key Tag usada pelo RRSIG RRs.
- O campo “Algorithm” lista o número do algoritmo RR DNSKEY referido pelo registro DS. O número algoritmo usado pela RR DS é idêntico ao algoritmo número usado por RRs RRSIG e DNSKEY.
- O campo “Digest Type” identifica o algoritmo usado para construir a digest.
- O Campo “Digest” é onde é calculado concatenando a forma canônica do nome do proprietário da RR DNSKEY com o RDATA DNSKEY.

Abaixo segue um exemplo do formato DS:

```
dskey.example.com. 86400 IN DNSKEY 256 3 5 ( AQOeiiR0GOMYkDshWoSKz9Xz
                                            fwJr1AYtsmx3TGkJaNXVbfi/
                                            2pHm822aJ5iI9BMzNXxeYCmZ
                                            DRD99WYwYqUSdjMmmAphXdvx
                                            egXd/M5+X7OrzKBaMbCVdFLU
                                            Uh6DhweJBjEVv5f2wwjM9Xzc
                                            nOf+EPbtG9DMBmADjFDc2w/r
                                            ljwvFw==
                                            ) ;  key id = 60485

dskey.example.com. 86400 IN DS 60485 5 1 ( 2BB183AF5F22588179A53B0A
                                            98631FAD1A292118 )
```

FIGURA: Exemplo Formato DS

FONTE: http://www.rfc-archive.org/getrfc.php?rfc=4034

- “dskey.example.com.”: especifica o nome do proprietário;
- “86400”: especifica o TTL;
- “IN DNSKEY”: especifica a classe e tipo de RR;
- “valor de 60485: é a chave para a tag correspondente "dskey.example.com". DNSKEY RR
- “valor 5” indica o algoritmo usado por "dskey.example.com" DNSKEY RR.
- “valor 1” é o algoritmo utilizado para construir a digest
- o resto do RDATA texto é o resumo em hexadecimal.

6 CONCLUSÃO

Com a crescente inovação tecnológica, acesso a sistemas e uso da internet, tornam-se cada vez mais fundamental assegurar a integridade, disponibilidade e o controle de acesso à informação em qualquer corporação, ou seja, manter a segurança do ambiente.

Mesmo com toda a tecnologia disponível no momento, é praticamente impossível obter segurança absoluta. Não existe um mecanismo único que forneça uma solução a esse tipo de problema; por isso, a segurança dos sistemas depende, em grande parte, da combinação de diversos fatores.

O serviço de DNS como já apresentado é extremamente importante dentro do cenário de funcionamento da internet, manter o serviço operante e de forma segura é o que o DNSSEC vem se aperfeiçoando para fazer, apesar de suas limitações seu desenvolvimento e utilização são um grande passo para manter o serviço de DNS.

REFERENCIAS

ALBITZ, Paul e LIU, Cricket; tradução de Izabel Cristina de Mendonça Santos. Um guia para administradores de Sistemas. **DNS and BIND**, Quarta edição. Sebastopol, California: O'Reilly and Associates Inc.: Editora Campus, 2001.

ALECRIM, Emerson. **O que é DNS (Domain Name System).** Disponível em: <http://www.infowester.com/dns.php> Acesso em 01 de março de 2011.

ARENDS, R. **Network Working Group - Request for Comments: 4034**. Disponível em: < http://www.rfc-archive.org/getrfc.php?rfc=4034> Acesso em 07 de novembro de 2011.

CAMPOS, David Robert Camargo de; JUSTO, Rafael Dantas. **Tutorial DNSSEC**. Disponível em: <ftp://ftp.registro.br/pub/doc/tutorial-dnssec.pdf>. Acesso em 10 de março de 2011.

CERT.BR. **Incidentes Reportados ao CERT.BR – julho a setembro de 2011**. Disponível em: <http://www.cert.br/stats/incidentes/2011-jul-sep/fraude.html> Acesso em 20 de Novembro de 2011.

COMPUTERWORLD.COM. **Como funciona o envenenamento de DNS**. Disponível em:< http://computerworld.uol.com.br/slide-shows/como-funciona-o-envenenamento-de-dns/paginador/pagina_1> Acesso em 25 de março de 2011.

DAVIES, Kim. **DNS Cache Poisoning Vulnerability.** Disponível em: <http://www.iana.org/about/presentations/davies-cairo-vulnerability-081103.pdf>. Acesso em: 08 de novembro de 2011.

DNSSEC.PT. **Porquê o DNSSEC?** Disponível em: < http://www.dnssec.pt/docs_pt/Porque_DNSSEC-Workshop_CERT.pdf> Acesso em 20 de Novembro de 2011.

MARIMOTO, Carlos E. **Instalando um Servidor DNS**. Disponível em: <http://www.hardware.com.br/tutoriais/instalando-servidor-dns/> Acesso em: 10 março de 2011.

MONTEIRO, Ricardo Vaz. **O que é DNS (e DNSSEC) bem explicadinho**. Disponível em: <http://webinsider.uol.com.br/2007/10/13/o-que-e-dns-e-dnssec-bem-explicadinho/> Acesso em 05 de marco de 2011.

_____. **DNS e DNSSEC for dummies**. Disponível em:<http://www.abraweb.com.br/colunistas.php?colunista=35&materia=77>. Acesso em 09 de Junho de 2011.

NEMETH, Evi. **Securing the DNS**.;login: The Magazine of Usenix & Sage, Nov. 2000, vol 25, nº 7. Disponível em: <http://www.usenix.org/publications/login/2000-11/pdfs/dns.pdf>. Acesso em: 05 de Junho de 2011.

NEVES, Frederico. **DNS - Por que DNSSEC agora mais do que nunca?** Disponível em: <ftp://200.160.2.8/pub/gts/gts12/05-PorqueDNSSEC.pdf> Acesso 10 de Novembro de 2011.

REGISTRO.BR. **FAQ (Perguntas Frequentes).** Disponível em: < http://registro.br/suporte/faq/faq8.html > Acesso em 20 de Outubro de 2011.

ROBERTS, Michael M. **Depoimento de Michael M. Roberts perante o Comitê para Comércio, Ciência e Transporte, Subcomitê para Comunicações, do Senado dos Estados Unidos da América**. Disponível em: <http://www.icann.org.br/correspondence/roberts-testimony-14feb01.htm> Acesso em 20 de Setembro de 2011.

ROHR, Altieres. **Ataque leva clientes do Virtua a site clonado de banco**. Disponível em: <http://g1.globo.com/Noticias/Tecnologia/0,,MUL1088103-6174,00.html>. Acesso em 08 de Novembro de 2011.

ROOT-SERVERS.ORG. **DNS clones espalhados pelo mundo**. Disponível em: http://root-servers.org/. Acesso em 15 de Abril de 2011.

ZILLI, Daniel. O Primeiro Livro do Mundo a Tratar do MaraDNS. **DNS por Daniel Zilli**. 1. ed. Rio de Janeiro: Editora Ciência Moderna Ltda., 2006.