SIMPOETS, CEFET-GO,161-171, 2008

Uma análise do protocolo DNS e suas extensões

Paulo Renato Lopes Seixas
Acadêmico de Sistemas de Informação
Universidade Estadual de Goiás - Unidade de Goianésia/GO
paulorenato@netsolution.eti.br

RESUMO: O estudo do protocolo DNS (*Domain Name System*) faz se necessário devido a sua grande importância para a estabilidade e confiança da internet que hoje conhecemos. O protocolo DNS nativo traz algumas vulnerabilidades intrínsecas em seu protocolo, tais como envenenamento de cache e impersonificação de servidores DNS. Hoje, temos uma extensão segura do protocolo DNS, denominado DNSSEC (*Domain Name System Security Extensions*), capaz de prover autenticidade nas requisições de DNS, garantindo assim a integridade dos pacotes DNS. Além desta extensão segura, existe outra denominada DNSCurve bem mais robusta porém consome mais recursos, devido todos os pacotes DNS utilizarem criptografia, desde sua origem até o destino.

Palavras-chaves: DNS, DNSSEC, DNSCurve, autenticidade, integridade

1 Introdução

A grande rede de computadores, a internet, é escalonável devido a existência do protocolo DNS, que permite a delegação de nomes de domínios para entidades e organizações sem haver a necessidade de um órgão centralizador, como existia na ARPAnet.

O DNS (Sistema de Nomes de Domínios) teve sua origem devido o crescimento da rede de computadores do Departamento de Defesa Norte-Americano, conhecido como ARPAnet. Nesta época havia apenas um arquivo denominado HOSTS.TXT que armazenava em um computador central todas as informações de mapeamento de endereços IP para nomes. Quando um computador tivesse a necessidade de obter um mapeamento atualizado, era necessário realizar o carregamento deste arquivo do servidor para o computador local, resultando em um grande fluxo de dados na rede de computadores e uma alta latência entre os computadores desta rede.

Desta forma, Mockapetris (1987) elaborou a RFC 1034 que especifica os conceitos e facilidades do protocolo DNS.

Tendo em vista a grande utilização do protocolo DNS em inúmeros aplicativos e sistemas, pode-se afirmar que o protocolo nativo DNS existe inúmeras vulnerabilidades intrínsecas. Com o objetivo de eliminar alguma dessas falhas, foi criado o DNSSEC – A extensão segura do protocolo DNS.

E de suma importância o uso desta nova extensão do DNS, pois permite a garantia de autenticidade, isto é, a origem de requisições DNS fazendo com que previna ataque de envenenamento de cache ou *main-the-middle*. Também garante a integridade dos

tipos de registros de recursos DNS e garante a não existência de um nome de domínio falso ou tipo de registro inexistente em sua base de dados.

O estudo do DNSSEC permite uma grande contribuição para a sociedade de uma forma geral, pois com este protocolo é possível tornar as aplicações cada vez mais seguras, tendo como exemplo, instituições financeiras que hoje são obrigadas a utilizar este protocolo em seus servidores de domínio, com o intuito de eliminar ataques de envenenamento de cache e transmitir confiança aos seus clientes.

Além da utilização do DNSSEC, temos o DNSCurve que é outra extensão segura do protocolo DNS, que realiza a criptografia de todos os registros de recursos DNS desde a origem da pesquisa até a sua resposta.

A motivação para a realização deste trabalho sobre segurança de redes de computadores, é demonstrar como é possível tornar as aplicações que utilizam do sistema de nomes de domínio, mais seguras e conseqüentemente tornar o ambiente da internet mais confiável através do uso de extensões seguras do protocolo DNS, como DNSSEC ou DNSCurve.

2 O protocolo DNS

O protocolo DNS (*Domain Name System*) é um sistema de nomes de domínio que realiza o mapeamento de endereços IP para nomes de domínio e vice-versa.

> A essência do DNS é a criação de um esquema hierárquico de atribuição de nomes baseado no domínio e de um sistema de banco de dados distribuídos para implementar esse esquema de nomenclatura. (TANEMBAUM, 2003, p.617).

Segundo Comer (2000) o DNS possui dois aspectos fundamentais, a saber:

11. O primeiro é abstrato, especifica uma sintaxe de nomes e regras para delegação de servidores de nomes autoritativos, isto é, que é responsável pelo domínio e todos os registros de recursos existentes na zona deste domínio.
12. O segundo é concreto, especifica a implementação e o sistema de computação distribuído que eficientemente realiza mapeamento de nomes para endereços IP (*Internet Protocol*). O DNS

> é um sistema de gerenciamento de nomes hierárquico e distribuído operando segundo duas definições: a primeira é examinar e atualizar seu banco de dados e a segunda é traduzir nomes de domínios em endereços de rede. (BARTH, s/d, p.1).

O protocolo DNS atualmente é um elo bastante forte para a tecnologia da informação. Observamos que através deste sistema de nomes de domínio é possível acessar sites sem haver a necessidade de inserir o seu endereço IP, e ao invés disso basta apenas sabermos o nome deste site. A parte robusta de realizar a tradução do nome de domínio para o endereço IP é feita pelo protocolo DNS.

2.1 Árvore DNS

O entendimento da árvore DNS e tão importante quanto o fundamento do protocolo DNS, pois é através da árvore do sistema de nomes de domínio que obtemos um registro de um domínio, a delegação de um domínio para a nossa entidade, ou a tradução de um nome de domínio para um endereço IP.

Segundo os autores Albitz e Liu (2006) o banco de dados distribuído do DNS é indexado através dos nomes de domínios (*Domain Name*). Cada nome de domínio pode possuir vários hosts, subdomínios e tem no máximo 127 níveis abaixo deste domínio. A árvore DNS pode ramificar em qualquer parte que haja uma intersecção no nó DNS, que é dividido pelo ponto (.).

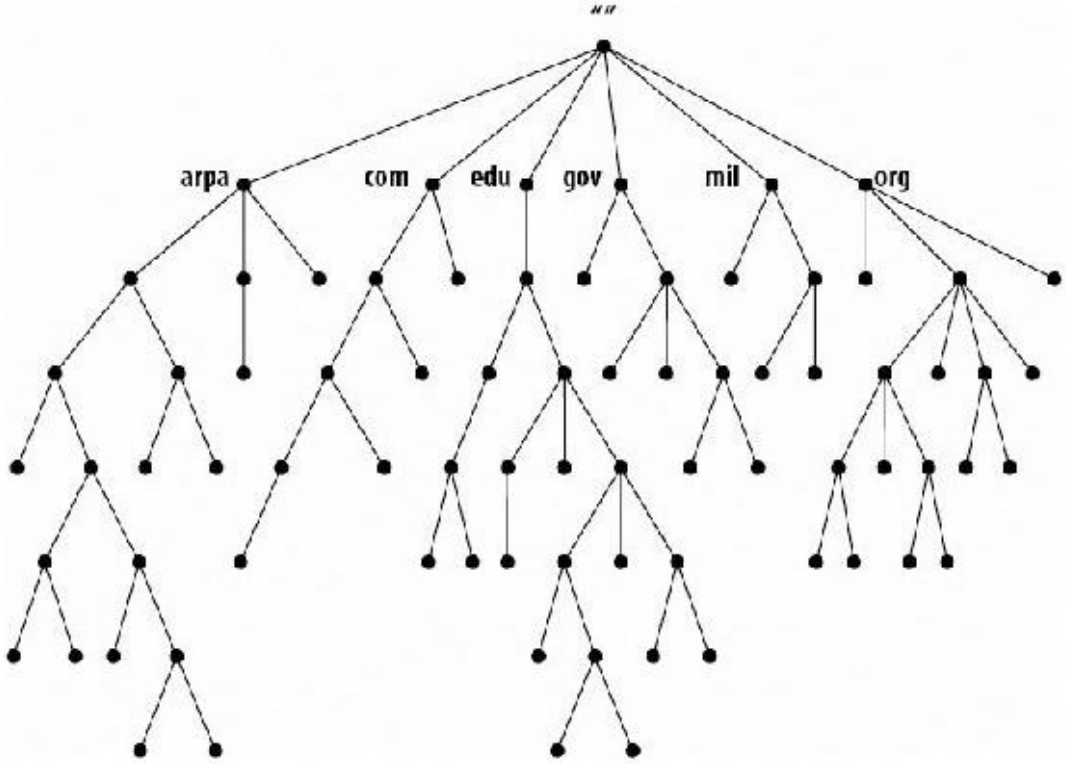

Figura 1. Representação da Árvore de DNS

O ponto (.) inicia a hierarquia do DNS, ele é conhecido como *root-servers*, em português, servidores raízes. Estes servidores possuem referência para todos os outros servidores DNS no mundo.

A tradução do nome de um web site, como

> howtos.linux.com será quebrado e resolvido começando por com, depois linux e finalmente howtos – itens chamados respectivamente top-level domain, second-level domain e third-level domain. É nessa ordem que o endereço IP para howtos.linux.com será obtido. (SIQUEIRA,2008,p.52)

A árvore DNS é o símbolo da estrutura hierárquica do sistema de nomes de domínio, por isto se torna muito mais fácil a sua administração, além do sucesso de ser escalonável.

2.2 Servidor raiz do Sistema de Nomes de Domínio

Conhecidos como *root-servers* são responsáveis por iniciar o nível hierárquico do sistema DNS, partindo do domínio raiz na qual é representado pelo ponto "." e suportado por vários servidores raízes. Estes servidores não respondem diretamente as requisições de pacotes DNS, ao invés disso realiza o encaminhamento para os servidores autoritativos, que são responsáveis pelas respostas ou encaminhamento para outro servidor DNS.

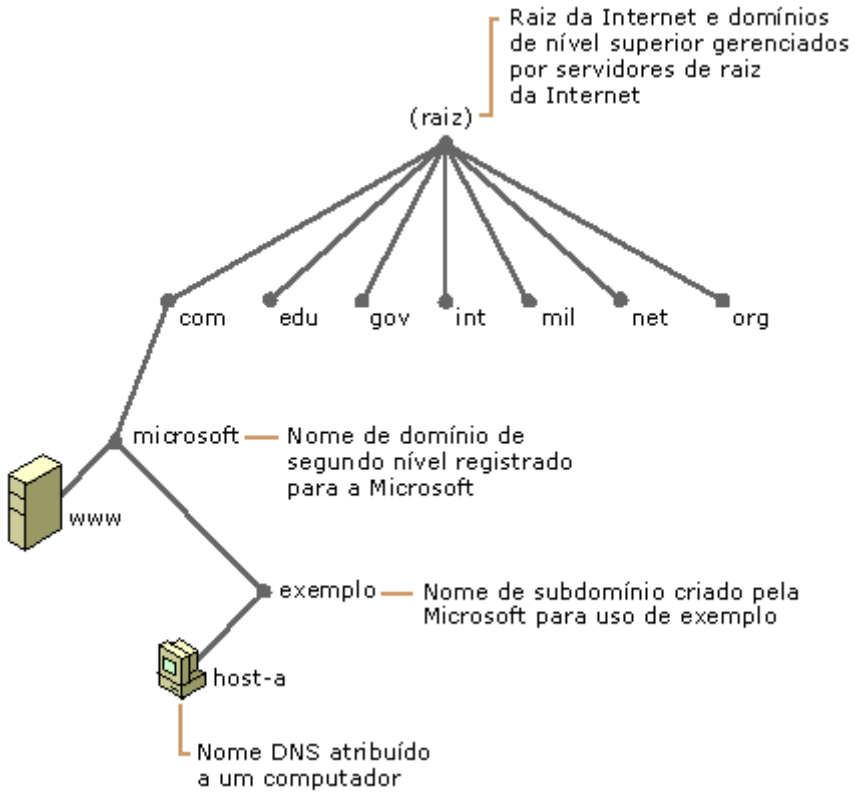

Figura 2. Hierarquia dos servidores DNS

raízes do IETF *Task* raizes de domínio para a Difusão e Segundo o (*Internet Engineering Force*), os servidores do sistema nomes de é o componente essencial internet. O Centro de de Tecnologia

Conhecimento informa, *on-line*, que existem 13 servidores DNS raiz no mundo todo e sem eles a Internet não funcionaria. Destes, dez estão localizados nos Estados Unidos da América, um na Ásia e dois na Europa. Para Aumentar a base instalada destes servidores, foram criadas réplicas localizadas por todo o mundo, inclusive no Brasil desde 2003.

Estas réplicas somente são possíveis graças ao compartilhamento do endereço IP *ANYCAST*. Ao todo, hoje existem 166 servidores raízes espalhados no mundo.

No Brasil existem réplicas destes servidores, sendo 01 servidor raiz, localizado em Brasília (*J.ROOT-SERVERS.NET*) e 02 servidores raízes em São Paulo (*F.ROOT-SERVERS.NET e J.ROOT-SERVERS.NET*)

Os servidores raízes possuem referência para todos os outros servidores DNS, por isso ele é responsável por iniciar a hierarquia do DNS.

Portanto, caso houvesse uma paralisação simultânea de todos os *root-servers*, a internet não funcionaria, não seria possível abrir qualquer web site na internet.

2.3 Registros de Recursos

Os registros de recursos são as peças fundamentais para popular o banco de dados do sistema de nomes de domínio. Os registros de recursos são contidos em arquivos de zonas, eles são responsáveis por informar qual tipo de mapeamento será feito para um determinado domínio.

Segundo, Nemeth, Snyder e Hein (2005, p. 306) “Cada zona de arquivo da hierarquia DNS possui um conjunto de registros de recursos associados a ela (o conjunto pode ser vazio)”.

2.3.1 Alguns tipos de Registros de Recursos

Segundo as RFCs (Request For Common) 882, 1035, 1183, 2065, 2181, 2308 e 2535 existem alguns registros de recursos que são muito importantes para a existência de um sistema de nomes de domínio eficiente.

Para Costa, os dados do serviço DNS

> são divididos em Registros de Recursos, ou abreviadamente RR. Esses registros compõem a menor unidade de informação disponível no DNS. Para uma mensagem DNS, os registros de recursos podem estar contidos nos campos Resposta e Complementar (COSTA, 2007, p. 30).

Tabela 1. Os principais tipos de registros de recursos

	Tipo	Nome	Função
Zona	SOA	*Start Of Authority*	Define uma zona DNS
	NS	*Name Server*	Identifica servidores de zonas, delega subdominios
Básicos	A	*IPv4 Address (32 bits)*	Mapeamento de nome a endereço (IPv4)
	AAAA	*IPv6 Address (128 bits)*	Mapeamento de nome a endereço (IPv6)
	PRT	*Point Record*	Resolução reversa (endereço-nome)
	MX	*Mai Exchange*	Controla o encaminhamento de e-mail
Segurança	KEY	*Public key*	Chave pública para um nome DNS
	NXT	*Next*	Usado com DNSSEC para respostas negativas
	SIG	*Signature*	Zona autenticada, com assinatura
Opcionais	CNAME	*Canonical Name*	Apelidos ou nomes alternativos para um host
	SRV	*Services*	Oferece as localizações de serviços

	TXT	*Text*	Comentários ou informações não transcritas, normalmente usado para registros SPF

3 Servidor Autoritativo

É o servidor que possui autoridade sobre um domínio qualquer, é capaz de responder as requisições DNS sobre o domínio com autoridade, isto é, informando que este servidor possui os arquivos de zonas com os registros de recursos solicitado do domínio em questão.

4 Servidor Recursivo

É o servidor que realiza um consulta recursiva, isto é, solicita informações sobre determinada requisição DNS em outros servidores, conhecidos como servidores autoritativos, até obter uma reposta satisfatória.

Segundo Campos e Justo (2008)

> Ao receber requisições de resoluções de nomes, o servidor recursivo faz requisições para os servidores autoritativos e conforme a resposta recebida dos mesmos continua a realizar requisições para outros servidores autoritativos, até obter a resposta satisfatória (p.13).

O servidor recursivo é obrigado a retornar uma resposta para o cliente DNS, seja positiva ou negativa.

5 Requisição de Endereços

É o mecanismo utilizado para realizar um consulta DNS. O Cliente deseja consultar o site www.sistemasabertos.com.br.

O cliente do DNS (*resolver*) irá realizar um consulta aos servidores de nome configurados no adaptador de rede deste computador. Logo, este servidor de nome recursivo irá fazer a consulta para os servidores raízes. Este servidor marca o início da cadeia de hierarquia do sistema de nomes de domínio.

Como os servidores raízes são servidores autoritativos e não respondem para todos os domínios, este irá apenas delegar a consulta DNS para os servidores de nome do domínio .br. Quando o servidor recursivo do cliente, realizar a mesma pergunta para os servidores de nome do domínio .br, estes irão apensas delegar a consulta para os servidores DNS do domínio .com.br até encontrar o servidor autoritativo do domínio sistemasabertos.com.br .

Ao encontrar o servidor de nomes do domínio sistemasabertos.com.br, este irá responder com autoridade a pergunta e informar o endereço solicitado para o cliente.

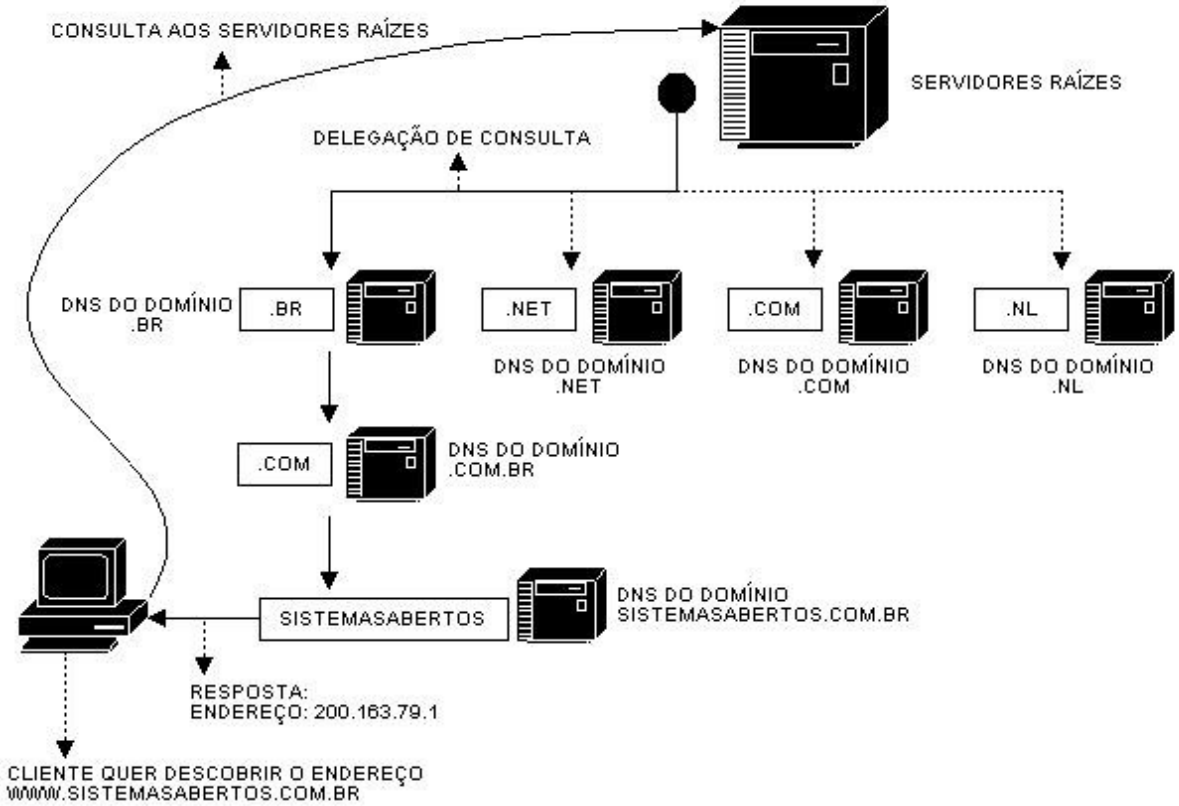

Figura 3. Resolução de endereços no sistema de nomes de domínio

6 Vulnerabilidades no protocolo DNS

Segundo o Registro.br as principais falhas no protocolo DNS são:

- A impersonificação do servidor recursivo, isto é, outro servidor DNS consegue “forjar” a identidade de um servidor recursivo original.
- Poluição ou envenenamento de cache, isto é, quando um intruso consegue falsificar as respostas DNS quando solicitada. Exemplo: O servidor recursivo faz a pergunta: Qual o IP do site “www.exemplodominio.com.br?” Para o servidor autoritativo do domínio exemplodominio.com.br, porém o intruso consegue responder mais rápido a solicitação do servidor recursivo, e portanto a resposta será falsificada e armazenada em cache no servidor recursivo, durante um tempo.

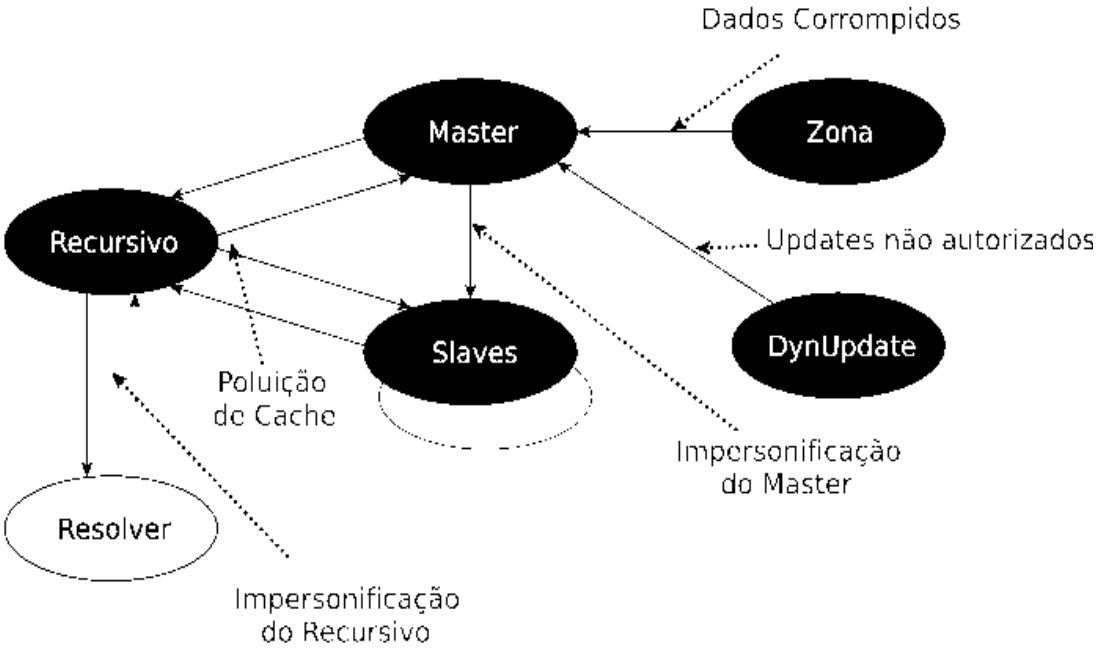

Figura 4. Vulnerabilidades no sistema de nomes de domínio

7 Extensão segura para o protocolo DNS: O DNSSEC

A extensão segura do sistema de nomes – DNSSEC resolve as principais vulnerabilidades no protocolo DNS, descritas acima.

O DNSSEC é uma extensão do protocolo DNS, logo o que já existe continuará a existir sem qualquer modificação. O DNSSEC tem o intuito de tornar mais seguro o protocolo DNS e oferecer esta mesma confiabilidade aos seus usuários da internet.

O DNSSEC hoje está em sua segunda versão, denominada DNSSEC bis.

Nemeth, afirma que

> DNSSEC é um conjunto de extensões DNS que autenticam a origem dos dados de zonas e verificam sua integridade usando criptografia de chaves públicas. Isto é, as extensões permitem que clientes DNS façam as seguintes perguntas: “Estes dados DNS realmente provêm do proprietário da zona?” e “Estes são realmente os dados enviados por este proprietário?”. (2004, p.329).

O DNSSEC provê a origem das requisições DNS, resultando na autenticidade dos registros de recursos de uma determinada zona.

Além de oferecer autenticidade os registros de recursos também fornecem integridade aos dados do sistema de nomes de domínio e demonstra se existe algum nome de domínio falso sendo requisitado ou algum tipo de registro de recurso que não exista em sua base de dados, o DNSSEC informa claramente caso não possua.

O DNSSEC utiliza-se do conceito de chaves assimétricas, sendo uma chave pública e outra privada.

Com o uso do DNSSEC, foram incorporados quatro novos registros de recursos ao DNS, eles são:

- DNSKEY – Chave pública;
- RRSIG – Assinatura dos registros de recursos;
- DS – Ponteiro para a cadeia de confiança;
- NSEC – Aponta para o próximo nome (Permite autenticar uma resposta negativa).

O DNSSEC não garante confidencialidade e negação de serviço (DoS).

7.1 Avanços da extensão segura DNSSEC no Brasil

Segundo o Registro.br todos os bancos e órgãos do poder judiciário são obrigados a utilizar DNSSEC no Brasil.

É obrigatório a execução do DNSSEC nos domínios .b.br e .jus.br . Hoje, no Brasil já existem 326 domínios registrados com DNSSEC.

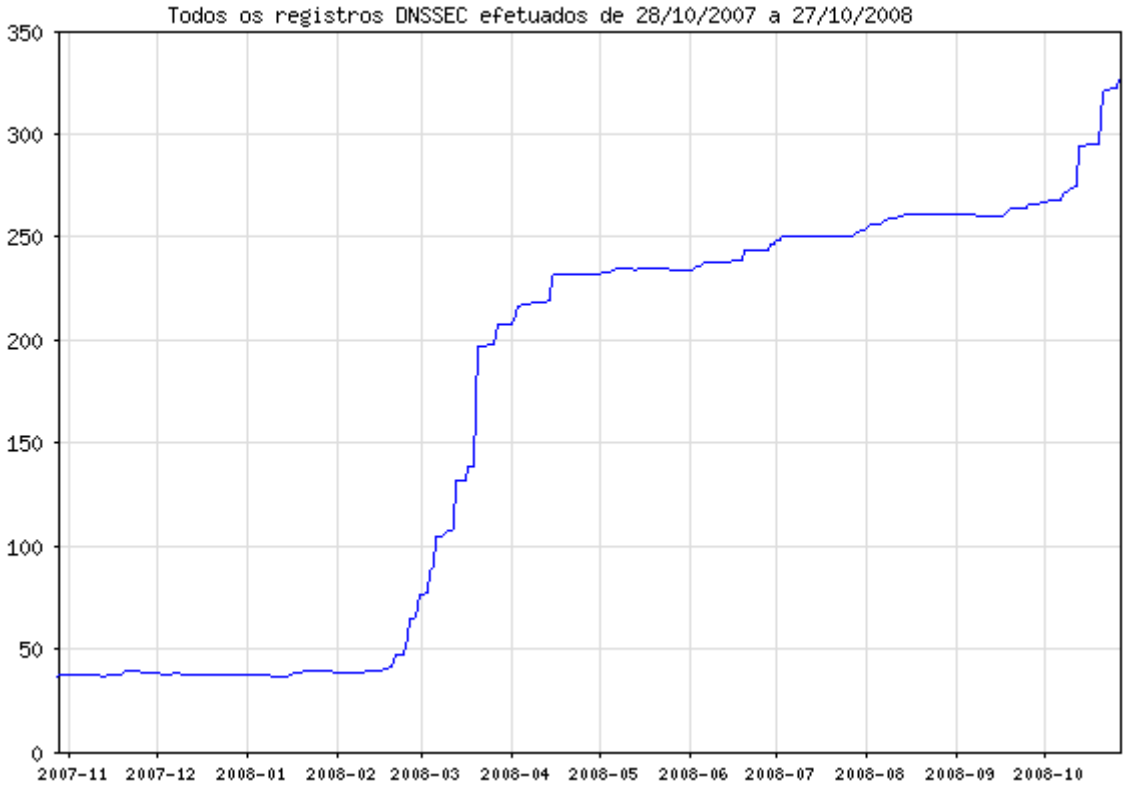

Figura 5. Registros DNSSEC efetuados no Brasil

8 DNSCurve

O DNSCurve utiliza criptografia de curva de elíptico de alta segurança que melhora drasticamente toda a dimensão de segurança do protocolo DNS.

DNSCurve oferece:

14. Confidencialidade

15. Integridade
16. Disponibilidade

Pode-se classificar o DNSCurve como um sistema tão eficaz quanto o DNSSEC, porém com o uso do DNSCurve, todos os pacotes DNS são criptografados, tendo como resultado a confidencialidade.

O DNSSEC não oferece confidencialidade.

9 Considerações Finais

O protocolo DNS é essencial para a sobrevivência da internet, contudo devemos sempre melhorar este protocolo, com à adoção de suas extensões seguras, como o DNSSEC e o DNSCurve.

O protocolo DNS acarreta consigo algumas vulnerabilidades que podem trazer grandes prejuízos para a sociedade de uma forma geral. Para evitar certos abusos neste protocolo, foi criado o DNSSEC – A extensão segura do protocolo DNS. Com esta extensão é possível eliminar as vulnerabilidades intrínsecas no protocolo DNS e consigo trazer mais segurança para todos os utilizadores desta extensão segura.

Contudo, observa-se que a adoção do DNSSEC no Brasil esta sendo feita de forma palatina, para os principais domínios de primeiro nível (DPN), tais como: eti.br, eng.br, adm.br, adv.br . Somente os DPNs .com.br e gov.br no momento não possuem suporte do DNSSEC. Segundo o Registro.br somente haverá suporte de DNSSEC nestes domínios quando a vulnerabilidade de varredura de zona no DNSSEC estiver totalmente corrigida.

Já a adoção do DNSCurve não é tão notória no Brasil, já que está acarreta um fluxo maior de dados entre as requisições DNS, devido todo e qualquer pacote DNS ser criptografado.

Referências Bibliográficas:

ALBITZ, Paul.; LIU, Cricket. *DNS and BIND***.** 5th Edition. United States of América: O'Reilly Media, 2006.

BARTH, Douglas Graciano.;SIEWERT, Vanderson Clayton. *Conceituação de DNS.* Santa Catarina. [2007?]. Disponível em: <http://artigocientifico.uol.com.br/uploads/artc_1148560980_24.pdf>. Acesso em: 10 agosto 2008.

CAMPOS, David Robert Camargo de.;JUSTO, Rafael Dantas. *Tutorial DNSSEC*. Disponível em:<ftp://ftp.registro.br/pub/doc/tutorial-dnssec.pdf>. Acesso em: 05 de outubro 2008.

COMER, Douglas E. Internetworking with TCP/IP. 4. ed. New Jersy: Printice Hall, 2000.

COSTA, Daniel G. *DNS: Um guia para administradores de Redes.* Rio de Janeiro: Brasport, 2006.

NEMETH, Evi.; SNYDER,Garth.;HEIN,Trent R. *Manual Completo do DNS*. Tradução Ariovaldo Griesi. Revisão técnica Mario Olimpio de Menezes.São Paulo: Pearson Makron Books, 2004.

SIQUEIRA, Luciano. LPI Nível 2: Aula 11. *Revista Linux Magazine*.v.42, p.52-58.2008.

TANENBAUM, Andrew S. *Redes de Computadores.* Tradução Vandenberg D. de Souza. 4. ed. Campus, 2003