UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANA
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZACÃO SOFTWARE LIVRE APLICADO A TELEMÁTICA

SÉRGIO LUIZ DE CARVALHO

DNSSEC – EXTENSÕES DE SEGURANÇA PARA SERVIDORES DNS

CURITIBA
2013

SÉRGIO LUIZ DE CARVALHO

DNSSEC – EXTENSÕES DE SEGURANÇA PARA SERVIDORES DNS

Monografia apresentada como requisito parcial para obtenção do grau de especialista em Software Livre Aplicado a Telemática, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná.
Orientador: Prof. Christian Carlos Souza Mendes

CURITIBA
2013

DEDICATÓRIA

Dedico esse trabalho a todos que de uma maneira ou de outra, contribuíram para que eu chegasse até aqui no meus estudos. Também aos meus pais como forma de agradecimentos e prova de reconhecimento a todo o esforço realizado para minha formação.

AGRADECIMENTOS

Agradecemos aos nossos familiares e amigos que nos deram o apoio necessário durante todas as faces desse curso especialização e na realização deste trabalho. Também a Universidade Tecnológica Federal do Paraná e todos os professores que contribuíram para nossa formação, em especial ao professor Kleber Kendy Horikawa Nabas e ao professor orientador Cristian Carlos de Souza Mendes que gentilmente participou desse projeto, também ás pessoas que passaram pelas nossas vidas, pelas amizades e pelos que não tivemos oportunidades de conhecer, que em algum dia podemos nos encontrar e enfim desfrutar de uma grande amizade.

EPÍGRAFE

“O primeiro passo em direção ao sucesso é o conhecimento.”

(Nicola Tesla)

RESUMO

O propósito deste trabalho constitui em divulgar informações sobre suas características e recursos do DNSSEC ”Domain Name System Security Extensions”, que é uma extensão do protocolo DNS que é um serviço responsável pelo processo de resolução de nomes e domínios da Internet. Neste contexto apresenta a importância do porque se motiva a sua utilização atualmente, também aborda as vulnerabilidades e falhas de segurança encontradas no antigo protocolo DNS, e relatando o porque sua indisponibilidade pode provocar na falta desse serviços na rede. Portanto, essa nova tecnologia o DNSSEC ela proporciona uma maior segurança no sistema de resolução de nomes reduzindo o risco na manipulação de dados e domínios forjados podendo ajudar a reduzir diversos problemas de segurança enfrentados pelos administradores de servidores. Por meio desta pesquisa que é exploratória pretendemos realizar uma comparação dessa tecnologia nova, buscando os resultados que possibilitem compreensão desse tema.

Palavras-chave: Protocolo DNS, DNSSEC, Segurança, Tecnologia, Redes.

ABSTRACT

The purpose of this paper is to disseminate information about its features and capabilities of DNSSEC "Domain Name System Security Extensions", which is an extension of the DNS protocol that is responsible for a service resolution process names and Internet domains. In this context the importance of features because it motivates its use today, also addresses the vulnerabilities and security flaws found in the old DNS protocol, and describing why their unavailability may result in lack of services in the network. Therefore, this new technology DNSSEC it provides greater system security name resolution in reducing the risk of data manipulation and forged domains can help reduce many security problems faced by server administrators. Through this exploratory research is that we will perform a comparison of this new technology, seeking results that enable understanding of this topic.

Keywords: Protoclo DNS, DNSSEC, Security, Techonology, Networks.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE SIGLAS

ARPANET	Advanced Research Projects Agency Network
BIND	Berkeley Internet Name Domain
CAIS	Centro de Atendimento de Incidentes de Segurança
DNS	Sistema de Nomes de Domínios
DNSSEC	Sistema de Nomes de Domínios Extensões de Segurança
DoS	Denial of Service
DMARC	Domínio de Relatórios Baseados em Mensagem de Autenticação
FTP	Protocolo de Transferência de Arquivos
HTTP	Protocolo de Transferência de Hipertexto
IANA	Autoridade para Atribuição de Números da Internet
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IP	Protocolo de Internet
ISO	Organização Internacional para Padronização
KEY	Chave
KSK	Key Signing Key
LANs	Rede Local
OSI	Organização Internacional para a Normalização
RFC	Request for Comments
RNP	Rede Nacional de Ensino e Pesquisa
RRs	Resouce Records (Registro de Recurso)
SIG	Assinatura
TCP	Transmission Control Protocol
TLD	TOP Level Domain
TSIG	Transction Signatures
TTL	Time To Live
UDP	User Datagram Protocol
URFJ	Universidade Federal do Rio de Janeiro
ZSK	Zone Signing Key

SUMÁRIO

1. INTRODUÇÃO

Esta pesquisa apresenta um abordagem sobe o tema do protocolo DNS e suas extensões de segurança o DNSSEC tem como objetivo ajudar atenuar um dos diversos problemas de segurança e vulnerabilidades que enfrentam os administradores de redes com DNS, mostrando uma comparação e sua importância na utilização. Durante a primeira década de sua existência as redes de computadores foram principalmente utilizadas por militares e Universidades e tendo com o objetivos de compartilhar e trocas de mensagens entre outros poucos recursos na época. Sob estas condições de uso a segurança nunca precisou de maiores cuidados, mas atualmente com crescimento de milhões de usuários na Internet há uma preocupação maior pois hoje utilizam essa rede de diversas maneiras novas, tais como por exemplo operações bancárias, operações de comércio eletrônico e acesso remoto ás informações confidenciais entre outas tantas.

Sobre o DNS podemos mencionar segundo Kurose (2008), afirma que o DNS é um banco de dados distribuído implementado em uma hierarquia de servidores de nomes, e um protocolo de camada de aplicação protocolo DNS, que permite que hosts consultem o banco de dados distribuído. E de modo segundo Tanenbaum (2003), demonstra que durante a década de 80 a Agência de Projetos de Pequisa Avançadas em Redes ARPANET, agência de pesquisa do governo norte americano criadora da rede originou a Internet começou a crescer rapidamente com a inserção de novas redes particularmente LANs. Com isso, a tarefa de localizar hosts tornou-se dispendiosa, e assim da necessidade de organizar as máquinas em domínios e mapear nomes de hosts em endereços IPs, foi criado o DNS.

> “A segurança das redes é uma preocupação diária de nível prioritário como consequência toda a redes pode sofrer falhas e problemas, essa estrutura de funcionamento do protocolo DNS tem sua importância mundial, conferindo que um grande alvo de terceiros mal intencionados para seu uso indevido ...” (ICANN, 2012).

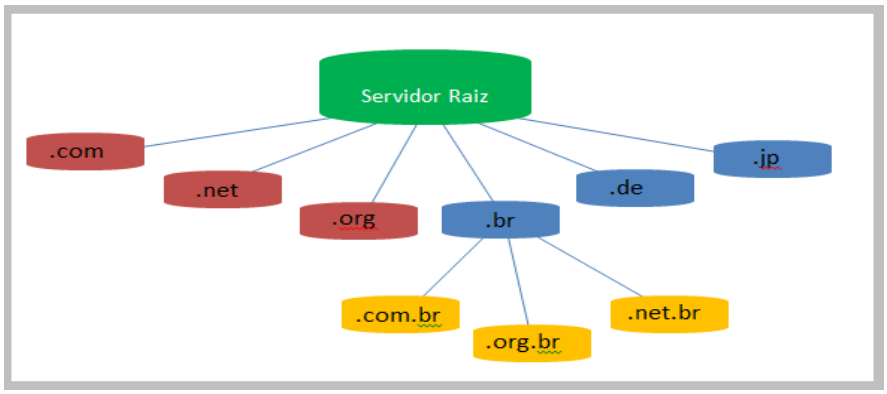
O DNS tem uma importância vital para operação adequada de quase todos os serviços na Internet, e comparação aplicação do DNSSEC na zona de raiz é a maior melhoria estrutural no DNS em vinte anos. A introdução do DNSSEC é um procedimento que teve amplo

envolvimento da comunidade técnica da Internet e está cuidadosamente dividida em estágios, de modo que seja possível identificar e solucionar imediatamente quaisquer efeitos indesejados (ICANN, 2010). Atualmente existe uma grande preocupação com segurança do DNS, a Rede Nacional de Pesquisas a RNP com seu Atendimento a Incidentes de Segurança CAIS informou em seu boletim um alerta de vulnerabilidade no ISC BIND intitulado "VU#800113" que trata de deficiências no protocolo DNS que permitem ataques de envenenamento de cache, pode fazer com que clientes de um servidor sejam direcionados par um host malicioso e ficar sobe o controle desse atacante.

Com esses problemas relatados, podemos mencionar o DNSSEC e uma alternativa importante na segurança segundo a entidade brasileira o Registro.br (2012), trata de um mecanismo de segurança previsto pela RFC2065 que propõem uma melhoria no sistema de autenticidade de resolução de nomes, reduzindo risco na manipulação dos dados e domínios forjados, visando suprimir as fragilidades do protocolo DNS. Deste modo, a utilização do DNSSEC propõem uma solução na atual tecnologia DNS. De acordo com Thompson (2002, p. 182), essa necessidade de proteção deve ser definida a partir das possíveis ameaças e riscos que a rede sofre".

Portanto, esta pesquisa tem objetivo de explicar funcionamento do DNSSEC que é composto de uma série de extensões ao protocolo DNS mostrando seus componentes, descrevendo as falhas e vulnerabilidades encontradas nessa tecnologia antiga do protocolo DNS, e apresenta a solução atual que esta a projetado para proteger a esses servidores de rede, pois sabendo o estrutura protocolo DNS e um dos principais mecanismo para funcionamento perfeito da Internet no mundo.

Figura 01: Detalhe da estrutura hierarquia do protocolo DNS



Fonte: adaptação do autor, 2012.

2. ORGANIZAÇÃO DO PROTOCOLO DNS

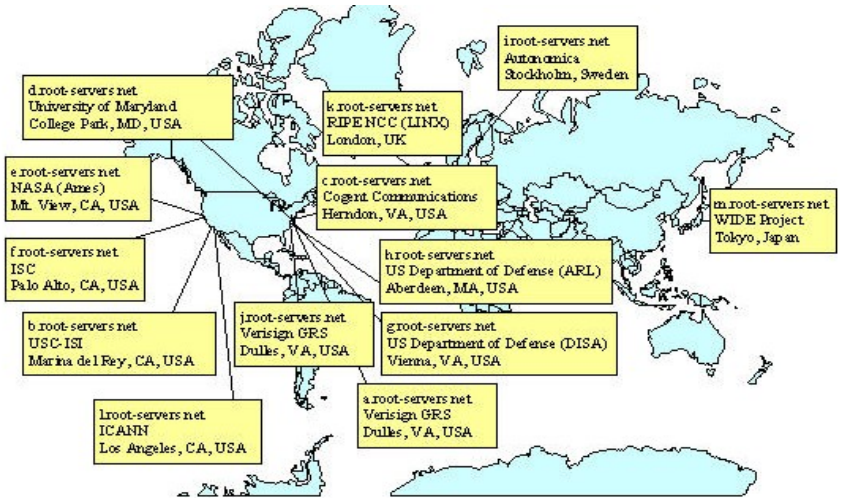
De acordo com a UFRJ (2012), a história teve inicio com Internet Network Information Center conhecido como IntetNIC, foi o órgão principal responsável por alocações de nomes e domínios entre 1972 até 1998, quando esse trabalho foi passado e assumindo pela entidade internacional ICANN junto a organização IANA. Mais antes no final da década 1960 e inicio 1970 a rede da ARPANET que tinha o objetivo principal de desenvolver uma rede de comunicação de interligar as bases militares e os departamentos de pesquisa do governo dos Estados Unidos para defesa, porém logo Universidades e outras Instituições relacionados tinham permissão para conectarem a essa rede.

O sistema da ARPANET resumia-se de algumas centenas computadores estava aumentando com tempo, esse sistema baseava no mapeamento entre nomes e endereços consistia num único ficheiro a tabela de Hosts.txt, que era mantido pela organização de Stanford Research Institute's Network Information Center “SRI-NIC”, a medida que novos computadores se ligavam na rede dessa época, o “ SRI-NIC” adicionava mais um nessa tabela, os administradores dos computadores ligados a rede tinham periodicamente atualizar os respectivos servidores de nomes de domínios, mas a medida que ia aumentando a computadores na rede a tarefa tornou-se complicado.

Embora funciona-se bem para o mapeamento entre nomes e endereços, não era forma mais prática, uma vez que essa rede estava em gigantesco progresso. Paul Mockaperis, da USC's Information Sciences Institute e outras pessoas decidiram criar em 1984, o sistema com RFCs 882 e 883 o DNS em substituição ao modo antigo de resolução de nomes, a grande vantagem deste novo sistema é que nenhuma entidade é a única responsável por sua atualização, o DNS baseiam-se no conceito de base de dados distribuída, existindo em muitos servidores de nomes diferentes em todo o mundo, isso permite assim um crescimento ilimitado do DNS, posteriormente foram produzidas as RFCs 1034 e 1035 em substituição as anteriores. Atualmente hoje dia existem 13 servidores DNS raiz no mundo todo, que são nomeados e conhecidos como Root-Serves e estão espalhados pelo geograficamente. Para aumentar a base destes servidores foram criadas réplicas, incluindo no Brasil, ficou determinado que cada servidor seria chamado por uma letra do alfabeto exemplo Server A, Server B assim por diante, e que pode m ser replicados em diversos lugares do mundo para

que o tempo de uma consulta tenha menor latência em relação a consulta ao próprio servidor (NORTHCUTT, 2001). A figura logo abaixo demostra a localização dos Roots-Servers no mapa no mundo.

Figura 02: Os 13 Root-Servers ao redor mapa do mundo.



Fonte: Adaptação do autor, 2012.

2.1 ESTRUTURA DO SISTEMA PROTOCOLO DNS

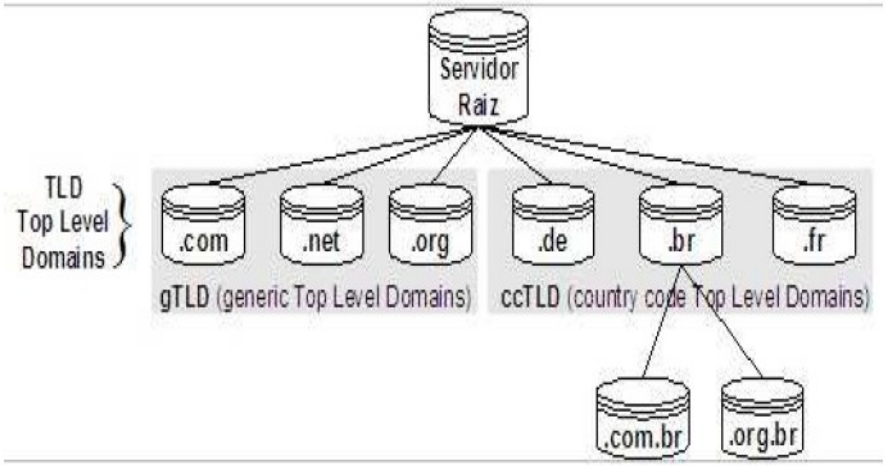
O servidor DNS (Domain Name Sytem) ele traduz nomes para endereços IP Internet Protocol em endereços IP para nomes respectivos, e permitindo a localização de hosts em um domínio determinado. Para cada domínio existe um registro no DNS que define qual o endereço IP do servidor de hospedagem e o IP do servidor de e-mail que responderão pro este domínio. É denominado resolução de nome ou resolução de domínio o processo que permite a descoberta do servidor que responde por um determinado domínio (TOPKE, 2000).

Com isso, por exemplo queremos acessar a página da Universidade Tecnológica Federal Paraná na Internet, o que fazemos é abrir um navegador qualquer e digitar o endereço www. utfpr.edu.br que é muito mais prático e fácil do que utilizar um endereço IP, como 200.203.194.66, mas poderia comentar que fácil decorar um enderenço de site que o usuário acessa várias vezes, mais imagine se tivéssemos que decorar enderenço IPs de todos os sites que acessamos na Internet não seria nada fácil. Porém, a comunicação com serviços como HTTP, FTP ou SMTP, por exemplo não é feita através de nomes mais sim através de endereços em forma numérica. Logo, precisamos de algum tipo de serviço que funcione como

um tradutor dos nomes em endereços numéricos vice-versa, esse tradutor é conhecido como sigla de DNS que é Sistema de Nomes de Domínios (RNP, 2012).

O DNS é uma base de dados hierárquica e distribuição entre milhares de servidores de DNS no mundo que tem como função converter endereços IPs de máquinas para nomes "reverso" e nomes de máquinas para endereços IPs. Mesmo numa rede local, sem conexão com a Internet, é usado para eliminar o problema de manutenção do arquivo no caso for Linux /etc/hosts, já que não precisa fazer nenhuma alteração nas máquinas que fazem parte da rede cada vez que for adicionada ou removida uma máquina da rede de um domínio. Mais ainda no caso, o /etc/hosts também não poderia conter todos os endereços utilizados no mundo. O sistema de nomes utilizado na Internet precisa ser escalável e suportar a definição de nomes únicos para todas as redes e máquinas na Internet e ainda permitir que a administração seja descentralizada. O que faz com que o DNS chegasse a esse nível foi principalmente foi a hierarquia. Dessa forma as informações foram divididas em níveis, e cada servidor DNS ficou responsável apenas por sua parte, essa estrutura tem o formato de uma árvore invertida, cujo topo é chamado de domínio raiz.

Figura 03: Estrutura dos Top Levels Domains (TLDs).



Fonte: Internet adaptação do autor, 2012.

Conforme mencionado na figura acima os servidores raiz tem uma tabela que indica qual o DNS será responsável e executor da resolução dos domínios para cada extensão de domínio nomeado de Top Level Domain TLD, possui também dois tipos Generic Top Level Domains gTLDs que são domínios genéricos usados no mundo todo e Country Code Top Level Domains ccTLDs extensões de domínios administrador pelos países. Ajustado aos

provedores de acesso das empresas de telecomunicação dos países ao redor do mundo em arquivar em seus caches a tabela dos 13 Roots-Serves eles não tem um grande volume de consulta. Pois essas consultas podem ser armazenadas em cache pelo DNS local por um período de tempo, para evitar ter um novo acesso externo. Isso só torna necessário uma nove consulta diretamente ao Roots-Serves quando uma nova TLD for criada, ficando responsáveis pelo um grande e maior volume de consultas aos servidores do Top Level Domains.

Quadro 01: Exemplos de ccTLDs e gTLDs.

ccTLD	País	*gTLD*	Entidade
.au	Austrália	*.biz*	Negócios
.br	Brasil	*.com*	Comércio
.ca	Canadá	*.edu*	Instituições de ensino
.de	Alemanha	*.gov*	Agências e entidades governamentais
.fr	França	*.jobs*	Publicação de vagas de emprego
.gr	Grécia	*.mil*	Organizações militares
.hk	Hong Kong	*.mobi*	Para sites voltados a dispositivos móveis
.jp	Japão	*.name*	Para nomes de pessoas
.uk	Reino Unido	*.org*	Organizações não governamentais

Fonte : Adaptação autor, 2012.

2.2 FUNCIONAMENTO DOS COMPONETES DO DNS

O Protocolo DNS basicamente de serve para mapear nomes em endereços IP, mais possui alguns elementos que são :

2.2.1 Os Clientes DNS

São chamados de Resolvers, são programas instalados nos computadores que estão responsáveis por perceber sempre que um programa precisa de resolução de nome e repassar esta consulta para um servidor DNS, estes Resolvers consultam o servidores de nomes, interpretam as respostas e retornadas pelo servidor e retornam as informações aos programas que os pediram e solicitaram. Quando uma aplicação precisa resolver um nome, ela é endereçada pelo Resolvers, então é iniciando um processo para esse nome. Em primeiro momento o endereço é passado ao cliente DNS, que tenta solucionar o nome utilizado no

cache do DNS local que esta no arquivo host. Quando um nome é resolvido com sucesso, o resultado é mantido na memória para que o cliente DNS utilize essas informações. Se o cliente DNS não encontra a resposta no cache, o cliente consulta as entradas no arquivo hots que é são o arquivo texto responsável pelos endereços IP.

Caso a consulta não seja certa após esses processos, o cliente DNS contacta o servidor local de nomes, mandando uma mensagem ao nome a ser resolvido com tipo de pesquisa a ser realizada e a classe associada ao nome DNS. Então, a espera que o servidor de nomes envie de volta uma mensagem de resposta ao DNS que contém a resposta da requisição. O Resolvers interpreta essa resposta que pode ser registro de erro, e envia para o programa que originou a requisição.

2.2.2 Registros de Recursos

Os dados são associados com nomes de domínios estão constitui dos registros de recursos os RR, esses são as entradas do banco de dados do protocolo DNS, que cada entrada existe um mapeamento entre um determinado nome da informação associada a esse nome. Podendo ser simples com endereço IP ou até mais complexo sofisticado, esses recursos definem os tipos de dados protocolo DNS e estão armazenados em formato de binário, mais quando consultados são enviadas pela rede em formato de texto, enquanto executam a transferência de zona, esse tipo de mensagem e divida em seções onde cada nome define os nomes do domínio dentro do espaço dos nomes de domínios. Detalhando a seção cabeçalho está sempre presente que inclui os campos que especificam quais as seções restantes estão presentes ao pacote protocolo DNS sempre e pesquisado uma resposta.

Os nomes das seções depois do cabeçalho são derivados do seu uso em uma pequisa básica. Esta seção question contém campos que descrevem a pesquisa para o nome só servidor, e são dos tipos da pesquisa “QTYPE” tipo de classe “QCLASS” e tipo do nome do domínio “QNAME”. A seção answer contém RRs com a resposta da pesquisa; a seção authority contém RRs que apontam para sevidores de nomes autoritativo e a seção additional records contém RRs que são relacionadas com a pesquisa. Logo abaixo detalhe mensagens protocolo DNS.

Quadro 02: Seções de mensagem protocolo DNS.

Cabeçalho	Descreve as outras seções e possui os 16 bits identificadores da consulta, o *query ID*.
Pergunta	Pesquisa para o servidor de nomes, contendo o nome, a classe e o tipo do conjunto de registros de recursos buscados, formando a resposta da consulta (RRset).
Resposta	RRs com a resposta da pesquisa. Sempre vazia ns consultas, contém o RRset que casa com a consulta, ou está vazia se o nome não existe, se foi feita uma consulta não recursiva ou se a consulta resulta numa referência (*referral*).
Autoridade	RRs apontador para servidor de nomes autoritativo. É sempre vazia nas consultas. Pode estar vazia em respostas. Se não estiver vazia, contém os RRs, NS e SOA da zona consultada. Isto é chamado, geralmente, de *referral data.*
Adicional	RRs informações adicionais. Também é sempre vazia em consultas e pode estar vazia em respostas.

Fonte: Adaptação do autor, 2012.

Registro de recursos do DNS tem 6 campos, veremos a seguir:

- NAME: Ele contém o nome protocolo DNS, e também tem uma referência ao seu próprio nome, para o qual o RR pertence.

- TYPE: É o tipo do RR que este campo é necessário, pois não é comum para um nome protocolo DNS ter mais de um tipo de RR. Os tipos mais comuns de RRs são os seguintes:

Quadro 03: São os principais registro de recurso.

Tipo de Registro	Descrição	Uso
A	Registro tipo endereço	Mapeamento de FQDN em endereço IP.
PTR	Registro tipo ponteiro	Mapeamento de endereço IP em FQDN.
SOA	Registro tipo *Start of Authority*	Especifica atributos referente à zona, como nome do domínio, contato administrativo, número de série da zona, TTL, etc.
CNAME	Registro tipo nome canônico	Nome de domínio canônico para um *alias* (nome alternativo).
MX	Registro tipo *Mail Exchange*	Nome do servidor de correio eletrônico para o domínio.
NS	Registro tipo *name server*	Define o nome do servidor da zona

Fonte: Adaptação autor, 2012.

- CLASS: São cada classe pertence a um tipo de rede ou software.

- TTL: Especifica o intervalo do tempo que o registro do recurso pode armazenar informações antes que a fonte da informação deva outra vez ser consultada.

- RDATA: O formato desse campo varia de acordo com o tipo e a classe do RR.

- RDATA Length: São tamanho em octetos do campo RDATA.

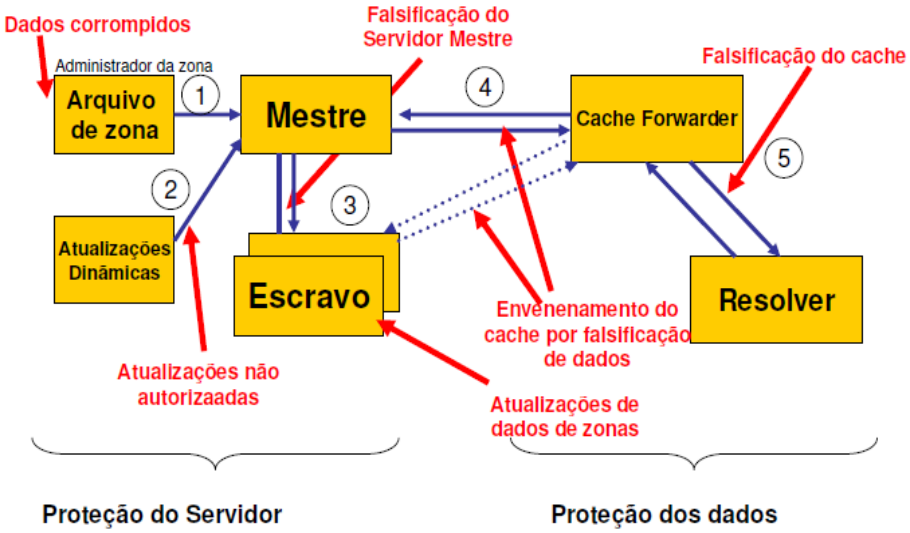
3. SEGURANÇA

De acordo com Soares (1995), para que uma política de segurança seja implementada existe a necessidade do cumprimento das regras definidas para o controle de acesso aos dados e recursos que trafegam pela rede da organização, definindo o que será ou não permitido a cada usuário dentro da hierarquia da rede, liberando ou não a utilização aos sistemas de comunicação de dados dessa organização. Com base na natureza da autorização que é dada ao usuário, pode-se dividir em dois os tipos de política de segurança existentes: uma baseada em regras, onde os dados e recursos da rede são marcados com rótulos de segurança apropriados que definem o nível de autorização do usuário que os está controlando, e uma outra baseada em identidade. Nesse último tipo, temos que o administrador da rede pode especificar explicitamente os tipos de acesso que os usuários da rede podem ter às informações e recursos que estão sob seu controle.

3.1 PRINCIPAIS PROBLEMAS DO DNS

Vamos mencionar alguns dos ataques mais conhecidos comuns sobre o protocolo DNS, são associadas riscos e vulnerabilidades dele, segundo site do Registro.br. Logo abaixo a figura ilustra em que ponto do fluxo da informações do DNS existem falhas se encontram.

Figura 04: Falhas no DNS.



Fonte: site Registro.br, 2012.

3.1.1 Ataques MITM

Os ataques main in the middle são ataques que permitem que um atacante em interceptar a rede com seu tráfego protocolo DNS ou forjar seu servidor DNS, a finalidade deste ataque é fazer o spoofing dos dados de entrada ou saída ou assumir a identidade do seu servidor original o DNS. Esse tipo de ataque o usuário atacante consegue ter acesso as informações importantes da infra-estrutura e do funcionamento da rede, bem como permite forjar respostas à varias vítimas sem o conhecimento da mesma spoofing. Uma segunda configuração interessante deste ataque é caso o atacante situe-se entre o servidor DNS primário e o servidor DNS secundário. Com isso, ele consegue obter informações detalhadas de todas as zonas das quais estes servidores DNS são responsáveis.

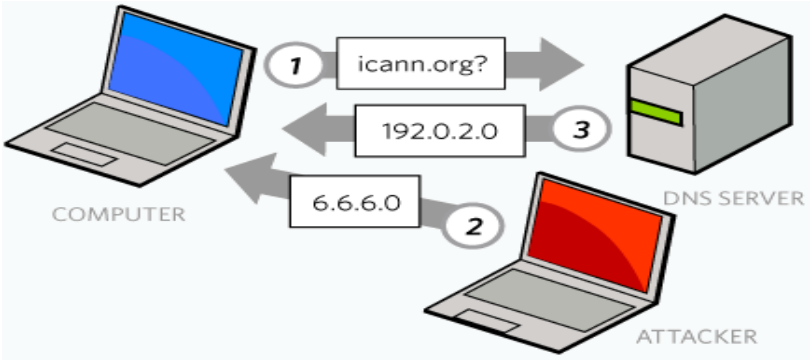
Figura 05: Ataque MITM "Main in the Middle".

Fonte: Adaptação autor, 2012.

3.1.2 Spoofing ao Protocolo DNS

Quando este tipo de ataque acontece tem a característica pela interceptação da rede e do tráfego do protocolo DNS, que através desta interceptação atacante substitui o tráfego original legítimo por pacotes DNS então forjados ao sua vontade e com isso consegue por exemplo, desviar o tráfego da vítima para um servidor falso. Esse servidor pode conter um site falsificado de uma organização por exemplo, este tipo desvio é conseguido através da resolução de nome, ao invés do cliente receber a resposta certa do site recebe como resposta falsa. Esse tipo de ataque não é uma tarefa difícil pois o protocolo DNS não é criptografado.

Figura 06: Ataque Spoofing ao Protocolo DNS.

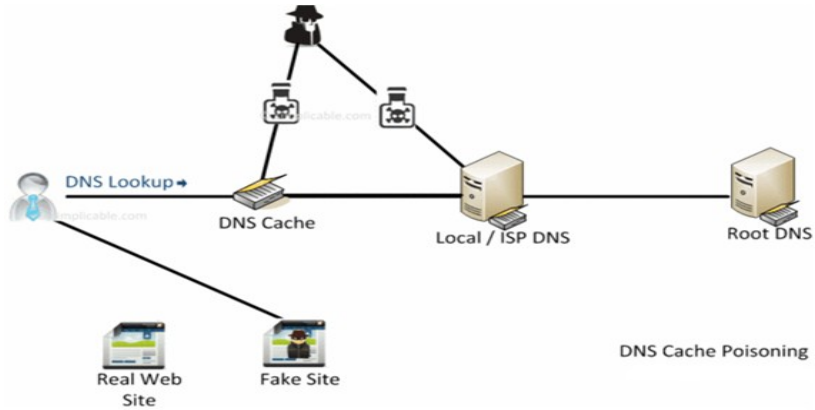


Fonte: Adaptação autor, 2012.

3.1.3 Envenenamento de Cache

Esse tipo de ataque ao DNS, é chamado de cache poisoning consiste em fornecer falsas respostas ao um servidor de cache DNS, antes que o verdadeiro servidor autoritativo responda a consulta realizada. A comparação principal entre o ataque do tipo spoofing de DNS e cache poisoning é que no segundo caso o atacante envia uma resposta falsa a um servidor recursivo, e não diretamente ao usuário, como no primeiro caso . Com isso, o servidor recursivo passa a armazenar resoluções protocolo DNS falsas em seu cache, então portanto quem resolve os endereços para um servidor falso. Com isso, o usuário ou cliente que solicitou a consulta dificilmente saberá que está acessando um site forjado.

Figura 07: Ataque envenenamento de Cache.

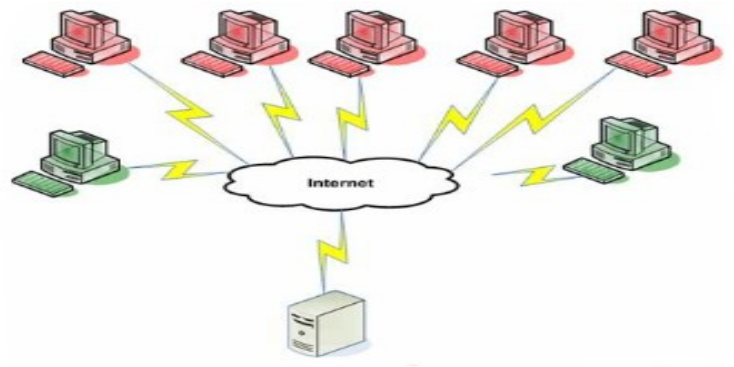


Fonte: Adaptação autor, 2012.

3.1.4 Ataques DoS e Ddos

Esse tipo de ataque ao DNS, é chamado de ataques de negação de serviço “DoS” consiste em deixar um servidor ou serviço indisponível, esse ataque consiste em inundar o servidor com um grande aumento de requisições de tal maneira que o servidor não consiga responder as consultas legítimas dos clientes, então o servidor fica inoperante e parado.Um outro objetivo também do ataque DoS é fazer com que o servidor autêntico por exemplo, o servidor DNS recursivo fique inoperante e seja substituído por um servidor falso, fazendo com que este assuma o lugar do servidor verdadeiro e responda as requisições destinadas a ele, esse ataque DoS parte de um máquina específica. Enquanto um ataque de negação distribuída “DDoS” pode ter como origem diversas máquinas até mesmo distantes entre si, o que dificulta muito mais o seu rastreamento específico.

Figura 08: Ataques DdoS.



Fonte: Adaptação autor, 2012.

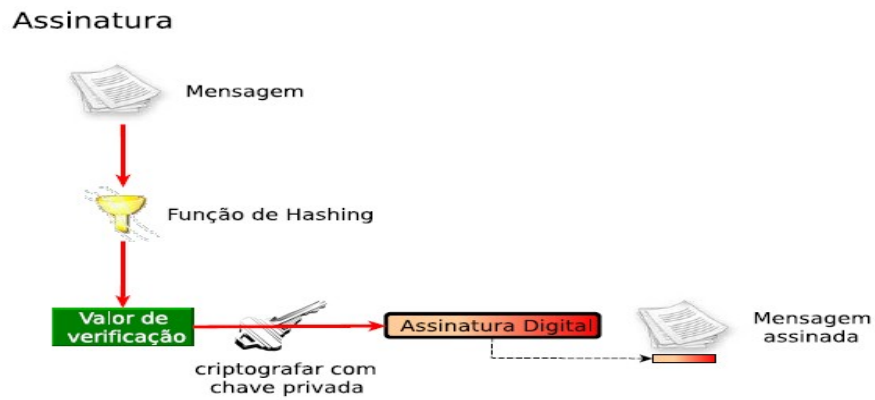
4. CONHECENDO AS EXTESÕES DNSSEC

O DNSSEC é um novo padrão que estende a antiga tecnologia do protocolo DNS, foi concebida para proteger e autenticar esse tráfego na rede, estas extensões fazem uso de criptografia que emprega assinaturas para autenticar e a integridade das informações trocadas entre os servidores DNS. Devido aos vários problemas e falhas encontrados no protocolo DNS, foi criada várias pesquisas relacionadas a segurança ao protocolo DNS, tendo a partir preocupação de eliminar essas ameaças nesse protocolo surgiu chamado de extensões de segurança o DNSSEC com a RFC 3833. Que descreve as principais características sobre DNSSEC como são integridade, autenticidade e a confidencialidade são os três principais pilares dessa tecnologia. A integridade é a garantia que os dados recebidos são exatamente idênticos como foram enviados não foram modificados ou corrompidos, inseridas novas informações ou excluídas, a confidencialidade trata da proteção da informação para que ela não esteja disponível a quem não seja de direito, e autenticidade dá garantias que a entidade se comunicando é quem realmente afirma ser (STALLINGS, 2008).

4.1 CONCEITO CHAVES NO DSSSEC

O DNSSEC tem por base a utilização de criptografia assimétrica, tecnologia com qual os dados são assinados, quando um domínio se encontra assinado, um servidor de nomes DNS pode autenticar as respostas que obtém protegido assim utilizando de algum ataques, como por exemplo, de informação corrompida na memória temporária do servidor.

Figura 09: DNSSEC utiliza o conceito de chave assimétrica.



Fonte: Site Regsitro.Br, 2012.

A criptografia assimétrica utiliza um par de chaves distintas, que são a chave pública e a chave privada. Tendo como as principais responsabilidades em relação de criptografia assimétrica no DNSSEC são:

1- Delimitação rigorosa das chaves privadas aos legítimos detentores;

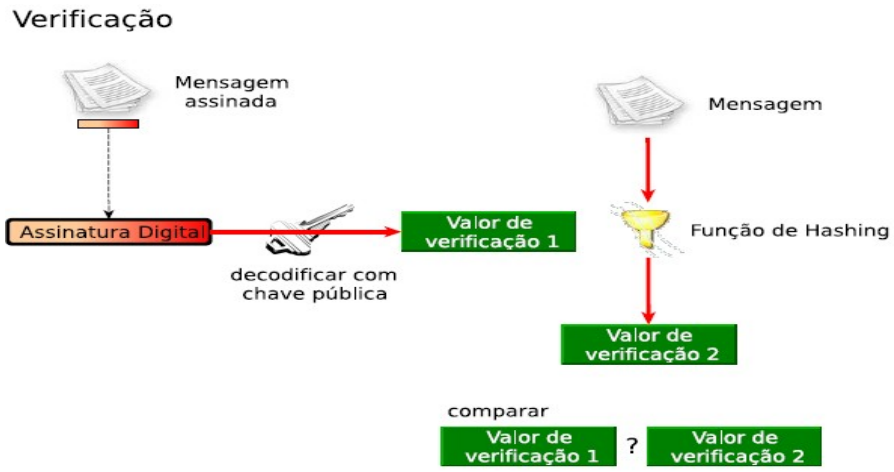
2- Distribuição confiável de chaves públicas a todos os que delas necessitam;

3- Atualização da informação da assinaturas da zona com a hierarquia superiores;

4- Correta manutenção da zona assinada;

5- Gestão do tempo de vida dos pares de chaves;

Figura 10: DNSSEC utiliza o conceito de chave assimétrica.



Fonte: Site Registro.br, 2012.

As chaves assimétricas são personalizadas, cada associado a pessoa, serviço ou servidores, o componente privado deve ser mantido em segredo devendo ser apenas do conhecimento e da utilização da entidade a que se encontra associado, a chave pública pode e deve ser publicamente divulgada para ser utilizada por qualquer entidade, sendo publicada no protocolo DNS na forma Resouce Record chamado DNSKEY. E utilizando a chave pública torna-se assim possível e validar uma assinatura que tenha sido gerada por uma chave privada, com o uso do DNSSEC foram incorporados quatro novos registros de recursos ao protocolo DNS que são:

1- DNSKEY – Chave pública, incluída na própria zona;

2- RRSIG – Assinatura dos registros de recursos RRset;

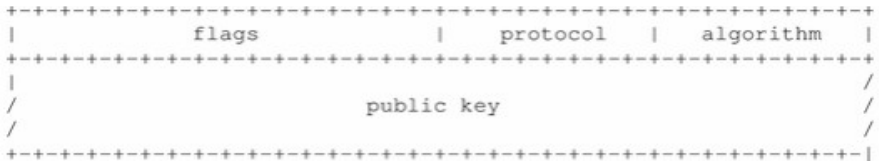
3- DS – Ponteiro para cadeia de confiança;

4- NSEC – Aponta para próximo nome, prova de não existência.

- Record DNSKEY

De acordo com tutorial do Registro.br (2012), trata-se de uma chave pública que válida as assinaturas digitais de um determinado domínio. Cada zona segura tem um par de chaves associadas a ela, os nomes a serem associados podem representar uma zona, uma máquina, um usuário ou uma outra entidade final. A chave pública do par de chaves da zona é publicada como um novo tipo de registro anexado ao nome de domínio da zona. O registro DNSKEY é usado para armazenar as chaves públicas que são usadas no processo de zonas DNSSEC, pelo uso da chave privada. O resolver pode autenticar a zona usando a chave pública para validar a assinatura contida no RRset.

Quadro 04: Representa a chave pública DNSKEY de uma zona.

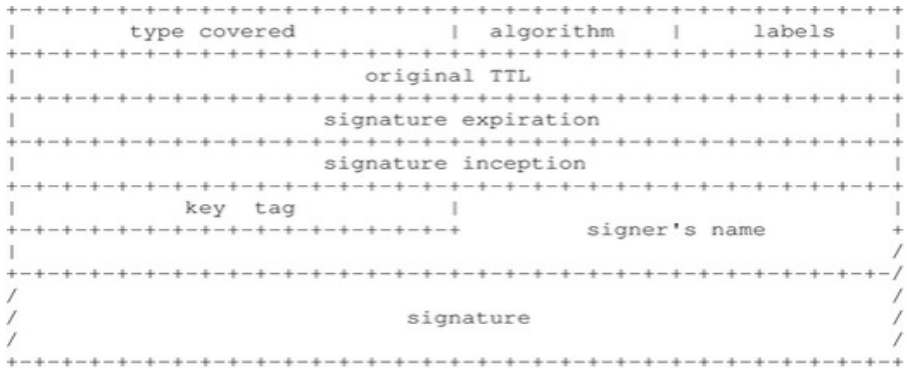


Fonte: Tutorial do Registro.br, 2012.

- Record RRSIG

Representa a assinatura de um RRset específica com uma determinada chave DNSKEY, possui uma validade inicial ” signature inception” e final “ signature expiration”.

Quadro 05: Parte específica do registro RRSIG.



Fonte: Tutorial do Registro.br, 2012.

- Record DS

Representa um hash de um record DNSKEY, indica que a zona delegada está assinada e também qual a chave e usada na zona delegada. O registro “delegation signer” o DS é envolvido na autenticação das zonas pai e filhas, forma uma cadeia de confiança a qual garante a chave e ancorada.

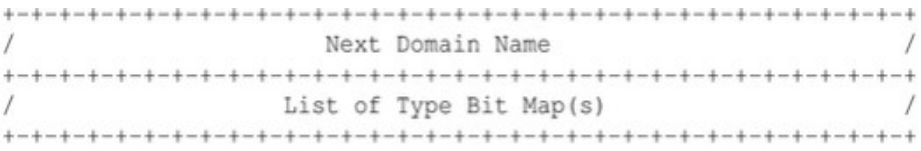
Quadro 06: Representa parte específica do registro DS.

Fonte: Tutorial Registro.br, 2012.

- Record NSEC

Permite autenticar uma resposta negativa, indica o próximo nome seguro na zona, também indica os tipos RRsets existentes para nome.

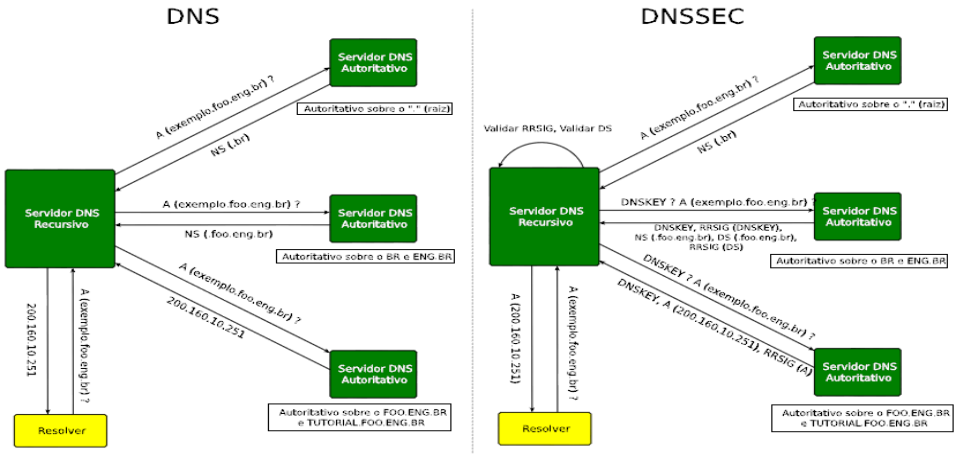
Quadro 07: Parte específica do registro NSEC.



Fonte: Tutorial Registro.br, 2012.

A figura abaixo, mostra a utilização os recursos do DNSSEC, e suas diferenças relação DNS.

Figura 11: Diferenças do uso entre uma requisição DNS e DNSSEC



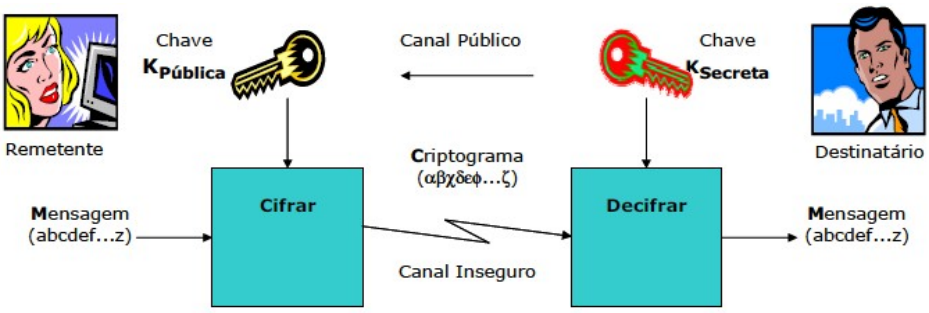
Fonte: Tutorial Registro.br, 2012.

4.2 GERÊNCIA DAS CHAVES

Tendo DNNSEC como o conceito de criptografia de chaves tem como definição a utilização de dois parâmetros de controles principal, por meio do qual a mensagem pode ser cifrada ou decifrada. Este par de chaves é gerado por meio de uma algoritmo de matemática, sendo assimétricas entre si, cada uma decodifica o que a outra codificou. O uso de certificados digitais garante a autenticidade do servidor e do usuário, e o uso de criptografia garante a confidencialidade e a integridade das informações. (THOMPSON, 2002)

De acordo com Kurose (2006), as técnicas criptográficas são meios que permitem que um emissor disfarce as informações os dados de modo que um intruso não consiga decifrar nenhuma informação, mesmo que estes dados sejam interceptados. Apenas o legítimo destinatário deve conseguir recuperar as informações disfarçadas . O DNSSEC usa assinaturas digitais por chaves públicas e privadas, de modo de não permitir a possibilidades de falhas, utilizando esses principio permite ao destinatário verificação da integridade e autenticidade de uma mensagem, e mostra se a informação foi alterada ou forjada por terceiros. Além de criptografar as mensagens, o DNSSEC também precisa certificar-se de que quem responde às consultas é realmente quem foi consultado.

Figura 12: Detalhamento do conceito chaves criptografada.



Fonte: Adaptação autor, 2012.

A manutenção de uma zona segura depende que as chaves devem ser trocada com alguma frequência, essa normalmente é sujeito a política de cada domínio, basicamente o DNSSEC utiliza dois tipos de chaves ”Key Signing Key” KSK e chave “Zone Signing Key” ZSK.

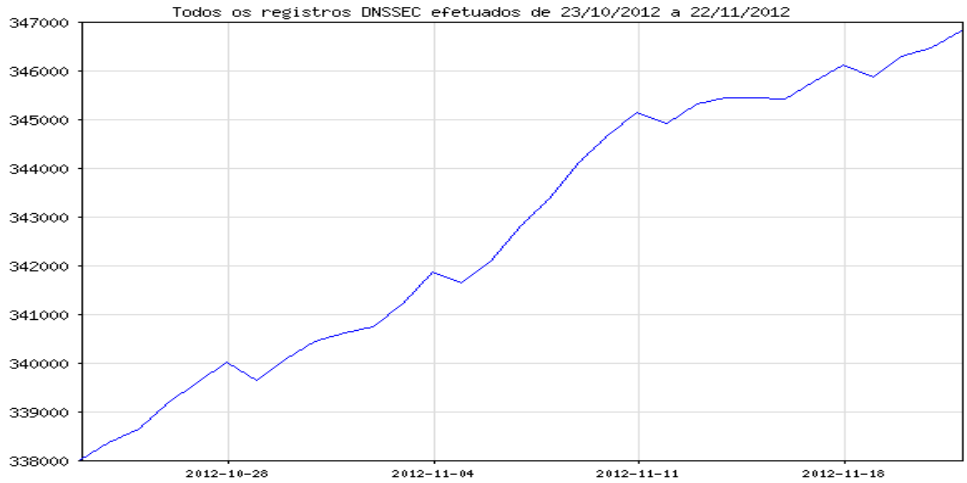
- Chave ZSK : essa chave utilizada para assinar zonas DNS, especificamente a zona .BR. este processo ocorre sempre que se efetua uma atualização ou geração de um novo arquivo de zona, esta chave é gerada pelo HSM e armazenada pelo próprio. Para além da versão original da chave que se encontrará armazenada no HSM é efetuada uma cópia de backup da ZSK para um “token” de segurança que é um dispositivo eletrônico seguro que armazena as chaves e que possui suporte para vários algoritmos de criptografia permitindo a existência, por razões de segurança, de uma cópia de reserva da chave no HSM e no “token” seguro e encriptado. O “token” de segurança com a cópia de reserva da chave KSK fica à responsabilidade da entidade externa.

- Chave KSK: é utilizada para assinar o conjunto de resource records DNSKEY que possuem a informação de todas as chaves contidas na zona. Uma vez que a KSK assina dados da zona, o seu tempo de vida de utilização pode ser mais extenso até à criação de uma nova chave. Esta é constituída por um par de chaves assimétricas a parte pública da chave é aquela que é publicada e comunicada pelos utilizadores da Internet, estabelecendo desta forma uma cadeia de confiança entre as várias hierarquias presentes no DNS. A chave KSK além de armazenada no HSM é ainda protegida num “token” de segurança permitindo tal no caso da ZSK da existência de uma cópia de reserva da chave no HSM. O “token” de segurança com a cópia de reserva da chave KSK fica à responsabilidade da entidade. Para a geração da KSK é utilizado o algoritmo RSASHA1 para NSEC3 com dimensão de 1280 bits.

5. INDICADORES DE USO DO DNSSEC

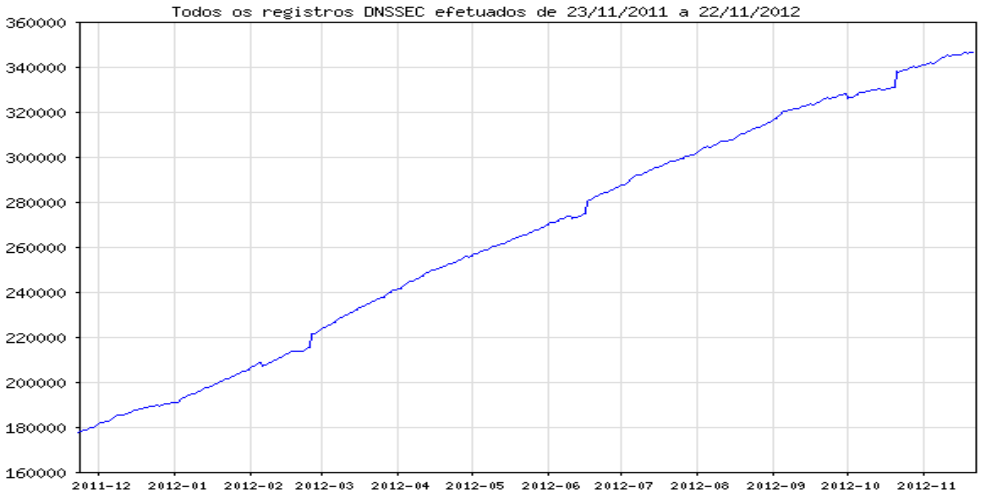
A utilização do DNSSEC vem aumentando a cada dia por se tratar e uma extensão que agrega ao protocolo DNS uma maior segurança, recomendado pelo “Internet Enginnering Task Force” IETF em suas publicações com suas soluções relacionadas as RFCs “Request for Comments”. Portanto, podemo e verificar através dos gráficos estatísticos do crescimento nos últimos anos e isso leva acreditar que poderá DNSSEC ser obrigatório futuramente. Os gráficos mostrados a abaixo estão atualizados no Site Registro.br.

Quadro 08: Crescimento da utilização do protocolo no último mês.



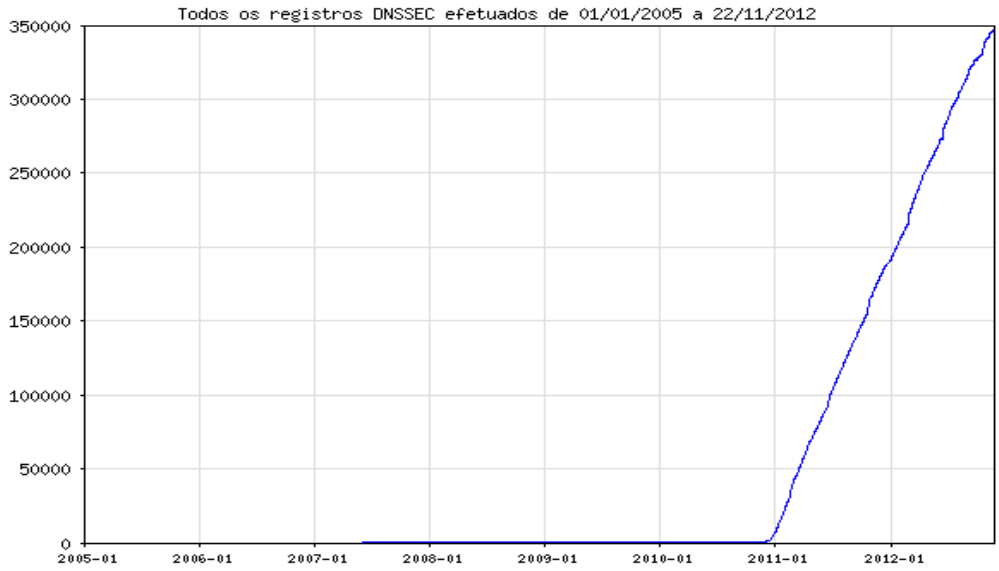
Fonte: Site Registro.br, 2012.

Quadro 09: Aumento protocolo no último ano.



Fonte: Site Registro.br, 2012.

Quadro 10: O crescimento da utilização do protocolo após surgimento país.



Fonte: Site Registro.br,2012.

Atualmente o Comitê Gestor da Internet órgão, que regula a grande rede no Brasil está a disposição essa nova tecnologia para os os sites do Poder Judiciário e os Bancos ligados a FEBRABAN a Federação Brasileira de Bancos estão a utilizando a extensão DNSSEC para sua segurança, com o propósito de evitar fraudes e não sofre algum risco segundo Demi Gestchko (2012), já são usados aqui mais de 20 mil deles. Somos os pioneiros no uso desse recurso, ao lado da Suécia. Nos Bancos são os únicos que podem utilizar o B.BR, no Poder Judicial JUS.BR que é de uso obrigatório, também pode ser usado em outros domínios com terminação ".BR". Todos esses avanços dessa tecnologia demonstra que esta sendo bem aceito no país. Entretanto, pesquisado em entidades internacionais tais como ICANN e IANA em seu plano estratégico de 2011 a 2014 estabelece seus objetivos global, de incentivar ainda mais especificação do DMARC com a propagação em adoção do DNSSEC no mundo, buscando a melhoria da especificas na segurança no protocolo DNS. No Brasil a empresa do provedores Hostnet e Infolink já disponibiliza o uso para seus clientes, o Cert-Bahia ligado a RNP mostra um artigo dando uma visão geral do DNSSEC no seu site.

6. PROCESSO PARA CONFIGURAÇÃO SERVIDOR

Agora vamos as configurações iniciais que descreve para implantação do DNSSEC, que serão listadas nesse roteiro.

6.1 ROTEIRO PARA CONFIGURAÇÃODE UM SERVIDOR AUTORITATIVO

-Verificar a disponibilidade do domínio junto a entidade Registro.br;

- Instalar BIND;

- Configurar um arquivo de zona no servidor Master;

- Configurar o arquivo Named.conf no servidor Slave;

- Executar o BIND no Named.conf no servidor Master;

- Executar o BIND no Named.conf no servidor Slave;

- Registrar o domínio na entidade Registro.br;

- Aguardar nova publicação;

-Realizar teste no servidor DIG;

- Criar chave KSK, DNSSEC-KEYGEN;

- Criar chave ZSK, DNSSEC-KEYGEN;

- Incluir as chaves geradas no arquivo de zona do servidor Master;

- Assinar a zona DNSSEC-SIGNZONE;

- Se existir delegações assinadas, inclui no arquivo de zona DS de cada delegação e reassinar mesma;

- Atualizar o Named.conf do servidor Master de forma a utilizar o arquivo de zona SIGNED e habilitar DNSSEC-ENABLE;

- Atualizar o Name.d do servidor Slave habilitando DNSSEC-ENABLE;

- Restartar o BIND o Name.d no servidor Master;

- Restartar o BIND o Name.d no servidor Slave;

- Adicionar na interface de provisionamento o DS, localizado dsset*;

- Aguardar publicação. (Registro.br, 2012)

6.2 ROTEIRO PARA CONFIGURAÇÃO DE UM SERVIDOR RECURSIVO

- Instalar biblioteca de desenvolvimento do OpenSSL;

- Instalar o BIND;

- Obter a trusted-key do site da entidade Registro.br;

- Configuarar arquivo Named.conf habilitando DNSSEC-ENABLE e DNSSEC-VALIDATION;

- Incluir a trusted-key no arquivo Named.conf;

- Executar o BIND. (Registro.br, 2012)

6. 3 TESTE NA CADEIA DE CONFIANÇA

- Instalar BIND com SIGCHASE;

- Obter a trusted-key do site Registro.br;

- Incluir a trusted-key no arquivo /etc/trusted-key.key;

- Realizar testes no servidor DIG mais SIGCHASE. (Registro.br, 2012)

CONCLUSÃO

Em resumo, esta pesquisa foi realizada podemos analisar e verificar que o sistema de nomes e domínios o protocolo DNS conta com bons resultados em termos de desempenho e disponibilidade no funcionamento da Internet, contudo devemos sempre melhorar este protocolo, assim devido as suas definições e características desse protocolo DNS contêm varias vulnerabilidade e falhas que podem levar sérias consequências como exemplo a falsificação das informação, redirecionamento do tráfego da rede e roubo de dados de usuários. De acordo com ICANN(2012), são realizados bilhões de resolução de DNS por dia em todo mundo, milhões de usuários utilizam Internet todo dia.

Desta forma, segundo os dados obtidos do entidade Registro.br existe um grande crescimento da escolha utilização DNSSEC nos servidores no Brasil demostrado nos decorrer desse trabalho. Em relação a segurança da extensão DNSSEC precisamos falar de sua necessidade, pois atualmente é uma das poucas tecnologias que tentam minimizar as falhas encontradas no protocolo DNS, sendo um projeto que caracteriza de implementação da criptografia assimétrica de gerências de chaves, para codificar as informações trocadas e garantir a sua autenticidade validando os dados e garantindo a sua origem impedindo qualquer ataques onde suas informação seja corrompida, essa segurança e descrito nas RFCs que tratam de detalhes específicos dessa operação.

Portanto, em se tratando desse sistema do protocolo DNS e sua extensão DNSSEC é um componente importante da cibersegurança, mas não é uma solução milagrosa, pois não resolve muitas das ameaças mais comuns relacionadas à insegurança da Internet como ataques DoS, enquanto principalmente existem inúmeros outros mecanismos e sistemas para ajudar a proteção e tornar qualidade da redes e servidores mais seguras para todos. Nesse pesquisa tratou-se em contribuir numa comparação do uso do DNSSEC, buscando influenciar para uma melhor conhecimento para essa opção de segurança, como sugestão de pesquisas futuras, sugere-se mais aprofundado sobre esse tema.

REFERÊNCIAS

ALBITZ, Paul; LUI, Cricket. **DNS e BIND**, 4a ed., Rio de Janeiro: Campus, 2001.

BRISA. **Arquiteturas de Redes com OSI e TCP/IP**, Makron. Rio de Janeiro: 1997.

CAIS: Centro de Atendimento a Incidentes de Segurança.**Vulnerabilidades no ISC BIND e outras implementações de DNS**. Disponível em:<http://www.rnp.br/cais/alertas/2008/uscert-vu8000113.html >Acesso em: 16 out. 2012.

CERT: Centro de Estudos Respostas e Tratamento de Incidentes de Segurança. **DNSSEC Adicionando mais Segurança no Sistema de Nomes e Domínio**. Disponível em: <http://www.pop-ba.rnp.br/Cert/DNSSEC_DocDetalhada> Acesso em: 11 out. 2012.

CERT: Serviço de Respostas a Incidentes de Segurança Informática. **Porquê o DNSSEC**. Disponível em: < http://www.cert.pt/index.php/rede-nacional-csirt/documentos > Acesso em: 05 set. 2012.

COMER, Douglas. **Interligação em Redes TCP/IP.** 3a.ed. Rio de Janeiro: Campus, 1998.

COMER, Douglas. **Redes de Computadores e Internet**. 2a.ed.Porto Alegre: Bookman 2001.

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

FEUP: Faculdade de Engenharia da Universidade do Porto. **Serviço DNS**. Disponível em: <http://paginas.fe.up.pt/~mgi97018/dns.html > Acesso em: 07 out. 2012.

DNSSEC: Protegendo o Sistema de Nome de Domínios com DNSSEC. **O que é DNSSEC**. Disponível em: < http://www.dnssec.net > Acesso em: 12 out. 2012.

DAVID, Robert. C. de C; JUSTO, Rafael. Dantas. **Tutorial DNSSEC.** Disponível em: <*ftp.registro.br/pub/doc/tutorial-dnssec.pdf* > Acesso em: 29 abr. 2012.

FERREIRA, Aurélio Buarque de Holanda. **Novo dicionário da língua Portuguesa**. Rio de Janeiro: Nova Fronteira, 1975.

ICANN: Corporação da Internet para Atribuição de Nomes e Números. **Aplicação do DNSSEC**Disponívelem:<http://www.icann.org.br/announcements/announcement-27jan10.htm > Acesso em: 21 set. 2012.

ICANN: Corporação da Internet para Atribuição de Nomes e Números, Plano estratégico 2011-2014.Disponivelem:<http://www.icann.org.br/announcements/announcement-7-21feb11.htm > Acesso em 21 out. 2012.

INFOLINK: Disponibiliza o DNNSEC para clientes no Brasil. Disponível em:< http://blog.infolink.com.br/dnssec-infolink-e-o-pioneiro-no-brasil-e-disponibiliza-a-delegacao-de-dns-seguro/> Acesso em 02 jan. 2013.

RNP: Rede Nacional de Ensino e Pesquisa. **Boletim Bimestral sobre Tecnologia de Redes**, Disponível em: <http://www.rnp.br/newsgen/9801/dnssec.html> Acesso em: 27 abr. 2012.

REGISTRO.BR. Registro de Domínio de Internet no Brasil. **Núcleo de Informações Coordenação do Ponto BR**. Disponível em: < http://registro.br/suporte/faq/faq8.html > Acesso em: 12 maio 2012.

STARLIN, G. **TCP/IP**: Internet, Intranet e Extranet. Rio de Janeiro: Book Express, 2001.

STALLINGS, W.**Redes e Sistemas de Comunicação de Dados**.Rio de Janeiro:Campus, 2005.

SOARES, Luiz. F. **Redes de Computadores**. 2a.ed. Rio e Janeiro: Campus.1997.

THOMPSON, M.A. **Proteção e Segurança na Internet**. São Paulo: Érica, 2002.

TANENBAUM, Andrew S. **Redes de Computadores.** 4a. Edição, Campus, 2003.

TÖPKE, C. R. P**rovedor Internet Arquitetura e Protocolos.**São Paulo: Makron Books, 2000.

UTFPR: Universidade Tecnológica federal do Paraná. **Normas para Elaboração de Trabalhos Acadêmicos**, Disponível em: <http://www.utfpr.edu.br/curitiba/biblioteca-e-producao-academica/normas-para-elaboracao-de-trabalhos-academicos > Acesso em 22 set. 2012.

UFRJ: Universidade Federal do Rio de Janeiro. **Como o DNS Trabalha**, Disponível em: <http://www.gta.ufrj.br/grad/anteriores98/dns-ticiana/works.htm#Tempo> Acesso em: 01 nov. 2012.

ROOT-SERVERS: Root Server Technial Operation. **Root DNSSEC**, Disponível em: <http://www.root-dnssec.org/2010/07/16/status-update-2010-07-16> Acesso em: 20 nov. 2012.

KUROSE, James F. e Ross, Keith W, **Redes de Computadores e a Internet uma Abordagem Top-Down**. 3.ed. Addison Wesley, 2006.