UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
CURSO DE ESPECIALIZAÇÃO EM TECNOLOGIAS, GERÊNCIA E SEGURANÇA DE REDES DE COMPUTADORES

ALESSANDRO CARBONI

Uma Análise do DNSSEC – Serviço de Nomes Seguro

Trabalho de Conclusão apresentado como requisito parcial para a obtenção do grau de Especialista

Prof. Dr. Raul Fernando Weber
Orientador

Prof. Dr. Sérgio Luis Cechin
Prof. Dr. Luciano Paschoal Gaspary
Coordenadores do Curso

Porto Alegre, dezembro de 2008.

AGRADECIMENTOS

Agradeço primeiramente a Deus que sempre me deu forças para lutar e acreditar nos meus objetivos, aos meus pais que sempre foram uma referência na minha vida em todos os sentidos e nos quais me espelho e tenho como porto seguro para os momentos de dificuldades, aos meus colegas que no decorrer do curso tiveram uma participação fundamental para que esse trabalho fosse concluído e a todas as outras pessoas que de uma forma ou outra me ajudaram para a conclusão do mesmo.

SUMÁRIO

LISTA DE ABREVIATURAS E SIGLAS

BIND	Berkeley Internet Name Domain
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
FEBRABAN	Federação Brasileira dos Bancos
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
KEY	Chave
NXT	Não Existe
RFC	Request For Comments
RR	Registro de Recurso
SIG	Assinatura
SO	Sistema Operacional
TCP	Transmission Control Protocol
TLD	Top Level Domain
UDP	User Datagram Protocol

LISTA DE FIGURAS

RESUMO

O objetivo do trabalho é dar uma pequena introdução ao uso de DNSSEC (*Domain Name System Security Extensions*) e ajudar a entender como a sua utilização pode ajudar a atenuar um dos diversos problemas de segurança que enfrentam os administradores de redes de grandes, médias e pequenas organizações. Como todo serviço de rede é suscetível a falha, a segurança com que as informações que trafegam pelos canais de comunicação entre as empresas e os clientes exigem que cada vez mais procedimentos sejam adotados, a fim de garantir a autenticidade das informações desde o seu início até o termino do processo. O que DNSSEC propõem é uma maior segurança no sistema de resolução de nomes, reduzindo o risco da manipulação dos dados e domínios forjados.

Baseado na tecnologia de criptografia que emprega assinatura, o DNSSEC utiliza um sistema de chaves assimétricas em sua tecnologia de trabalho. A sua utilização vem crescendo vertiginosamente no último ano e isso leva a acreditar que poderá até mesmo ser a referência utilizada para resolução de nomes, visto que, no estágio atual, a certificação pelo nome usando o DNS (*Domain Name System*) é altamente insegura.

A RFC 2065 (*Request For Comments*) é a referência para quem for aprofundar mais o assunto e leva a demais bibliografias que servem de fundamentação ao tema.

Palavras-Chave: DNSSEC, DNS, Protocolo Seguro, Resolução de Nomes.

An Analysis of DNSSEC – Service Security Names

ABSTRACT

The objective is to give a short introduction to the use of DNSSEC (Domain Name System Security Extensions) and help understand how its use can help alleviate one of several security problems faced by administrators of networks of large, medium and small organizations. Like any network service is susceptible to failure, security with that information that travel the channels of communication between businesses and customers increasingly require that procedures be adopted to ensure the authenticity of the information from its inception until the end of the process. What DNSSEC is proposing increased security in the name-resolution system, reducing the risk of manipulation of data and domain forged.

Based on encryption technology that employs signature, the DNSSEC uses a system of asymmetric keys in their technology work. Its use has grown very fast in the last year and this leads to believe that it may even be the reference used for name resolution system, since the current stage, the certification by name using the Domain Name System (DNS) is highly insecure.

The RFC 2065 is the reference for those over furthering the matter and leads to other bibliographies that are the subject of reasoning.

Keywords: DNSSEC, DNS, Security Protocol, Name-Resolution System.

1 INTRODUÇÃO

Durante a primeira década de sua existência, as redes de computadores foram principalmente usadas para pesquisas acadêmicas, por militares e por funcionários de organizações com o objetivo de compartilhar documentos, troca de mensagens, compartilhamento de impressão entre outros recursos. Sob estas condições de uso restrito, a segurança nunca precisou de maiores cuidados. Mas atualmente, como milhões de pessoas estão usando as redes para executarem operações bancárias, operações de comércio eletrônico e acesso remoto às informações confidenciais, a segurança das redes de informação é uma preocupação diária de nível prioritário dentro de qualquer organização. (TANENBAUM , 1997)

A autenticação é o processo de identificar com quem está se trocando informações sigilosas, ou seja, é o processo de confirmação se o destinatário é realmente quem você desejou contatar.

Na vida real podemos identificar outras pessoas através de suas feições, características e demais semelhanças que são percebidas aos olhos, e as comprovações são feitas através de assinaturas em contratos ou qualquer meio que caracterize um compromisso firmado, com símbolos em alto relevo e através de outras formas de reconhecimento. Geralmente as falsificações são detectadas por especialistas em caligrafia, papel e tinta. Infelizmente estas opções não estão disponíveis no mundo digital, por isso está muito claro que são necessárias outras soluções.

Basicamente as redes de computadores não são seguras. Existem muitas soluções para se implementar segurança em uma rede. Pode-se escolher dentre varias opções; ações implementadas desde ao nível da camada física até ao nível da camada de transporte, pois existem possibilidades variadas de tecnologias para segurança. (COMER, 2001)

Uma das soluções mais adotadas visando manter o sigilo das informações enviadas em uma rede de dados consiste no uso da criptografia, ou seja, as informações são embaralhadas de tal maneira que só os computadores autorizados consigam resgatar a informação na sua forma original. (THOMPSON, 2002)

O DNSSEC (*Domain Name System Security Extensions*) é um mecanismo proposto para tornar o protocolo DNS (*Domain Name System*) seguro. É composto de uma série de extensões ao DNS, a qual fornece autenticação e integridade fim a fim e foi projetado para proteger a internet de certos tipos de ataques, como DNS spoofing.

Todas as respostas as requisições no DNSSEC são digitalmente assinadas. E através da verificação da assinatura, o resolver pode checar se a informação é idêntica a mantida pelo servidor autorizado.

O DNSSEC estabeleceria um selo à prova de falsificações para as aplicações como Web e E-mail. Hoje em dia, os *hackers* e *spammers* personificam fontes de informação da Internet de forma relativamente fácil. O DNSSEC pode aumentar a probabilidade de que um email é na verdade do domínio a qual indica e que a informação obtida de um servidor Web é realmente advinda do site Web desejado e não de um impostor.

Hoje é possível redirecionar as requisições HTTP (*Hypertext Transfer Protocol*) ou FTP (*File Transfer Protocol*) para domínios forjados através dos servidores maliciosos de DNS. (FALBRIARD, 2002)

2 DNS E DNSSEC

2.1 DNS (*Domain Name System*)

Para que se possa visitar uma pagina Web ou quando pretende enviar uma mensagem eletrônica, o navegador ou o cliente de e-mail precisa saber em qual servidor essa pagina está hospedada e o e-mail esta armazenado para poder responder à sua solicitação. Esta informação sobre a localização dos servidores fica armazenada em servidores chamados DNS (*Domain Name System* – Sistema de Nomes de Domínios).

O servidor DNS traduz nomes para os endereços IP (*Internet Protocol*) e 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 por 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. (TÖPKE, 2000)

Todo o processo de resolução de nomes que ocorre para que uma mensagem seja enviada ou uma página Web seja acessada não é transparente para o usuário. Ele apenas sabe que sua solicitação foi atendida.

Por medida de segurança, um domínio pode definir vários servidores DNS, sendo sempre o servidor DNS primário o primeiro sistema a ser consultado para tentativa de resolução de nome e caso o mesmo venha a falhar ou não estar disponível entra em ação o próximo servidor de consulta que é o servidor DNS secundário uma espécie de cópia de segurança do servidor DNS primário e continua assim sucessivamente até que se obtenham a resposta solicitada. (STALLINGS, 2005)

O protocolo DNS utiliza o protocolo de transporte UDP (*User Datagram Protocol*) para as tradicionais requisições devido ao baixo *overhead* e melhor desempenho. E utiliza o protocolo TCP (*Transmission Control Protocol*) para a funcionalidade de transferência das zonas. (STALLINGS, 2005)

A estrutura do banco de dados DNS é um sistema de gerenciamento de nomes distribuído e hierárquico, ao invés de um banco de dados central e único, a resolução ocorre consultando diversos servidores DNS e sua resolução é hierárquica. A estrutura hierárquica é equivale a uma árvore invertida, existindo um servidor principal que aponta para um secundário que aponta para um terceiro e assim sucessivamente. Em virtude do banco de dados de DNS ser distribuído, seu tamanho é ilimitado e o desempenho não degrada tanto quando se adiciona mais servidores nele. O servidor DNS que está no topo da internet é o servidor raiz.

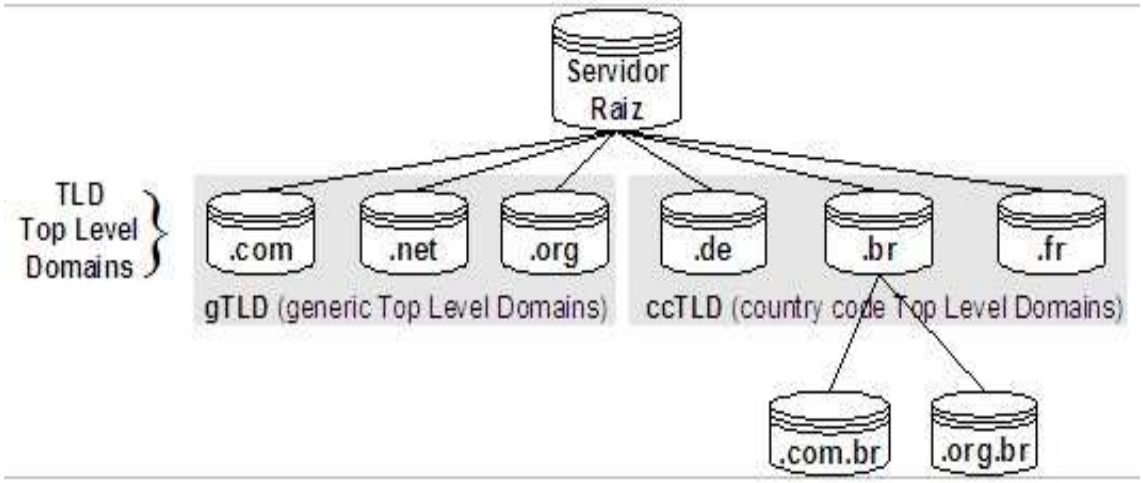


Figura 2.1: Servidor DNS

Servidor raiz

O servidor raiz da internet possui uma tabela que indica qual DNS será responsável pela resolução dos domínios para cada extensão de domínio TLD (*Top Level Domain*) diferente.

A tabela em si é muito pequena, possui apenas uma entrada para cada TLD existente. Os TLDs são de dois tipos: gTLDs (*Generic Top Level Domains* - domínios genéricos usados no mundo todo) e ccTLDs (*Country Code Top Level Domains* - extensões de domínios administrados pelos países).

Existem 13 servidores DNS raiz no mundo todo, que são conhecidos como *root servers*, 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. Ficou convencionado que cada servidor seria chamado por uma letra do alfabeto (*Server* A, *Server* B e assim por diante) que podem ser replicados em diversos lugares do mundo para que o tempo de uma consulta tenha menor latência em relação à consulta ao próprio servidor. A imagem a baixo representa a localização dos *root servers* e suas cópias espalhadas pelo mundo. (NORTHCUTT, 2001)

Figura 2.2: Imagem dos *root-servers*

Devido aos provedores de acesso e as empresas de telecomunicação ao redor do mundo arquivar em seus caches a tabela dos *root-servers* eles não tem um volume de consulta tão grande assim. Essas consultas podem ser armazenadas em cache pelo DNS local por um período de tempo, para evitar um novo acesso externo. Isso só torna necessária uma nova consulta diretamente ao *root-server* quando uma nova TLD for criada, ficando responsáveis pelo maior volume de consultas os servidores de *top level domains*.

2.2 DNSSEC (*Domain Name System Security Extensions*)

Como visto na Seção 2.1, o DNS é responsável por traduzir nomes de domínios para seus respectivos endereços IP. Como todo serviço de rede, é suscetível a falhas de segurança, a partir de agora que será dada a abordagem sobre o trabalho realizado focando na importância que a segurança oferecida pelo DNSSEC adiciona ao sistema de resolução de nomes o tornando mais seguro, reduzindo o risco de manipulação de dados e possibilidade de domínios serem forjados.

O envenenamento de cache do DNS é um tipo de ataque específico que o DNSSEC previne. Essa falha de segurança na estrutura hierárquica de resolução de nomes, onde um DNS aponta para outro DNS, possui um problema intrínseco de segurança, abrindo

a possibilita de um criminoso redirecione um site de banco, por exemplo, para um servidor próprio, onde todas as informações que o usuário envia seriam recebidas pelo golpista, inclusive informações como agência, conta e a senha do um determinado cliente. Para não repetir a consulta toda vez que um usuário requisita acesso a um determinado site, o servidor DNS armazena as informações em um cache, podendo permanecer por até três dias até que uma nova resolução de nome seja feita e o cache seja limpo daí vindo o nome de envenenamento de cache.

Os novos serviços disponibilizados pelo DNSSEC propõem três serviços distintos sendo a distribuição de chaves, a certificação da transação e requisição e a certificação da fonte de origem dos dados.

As extensões apresentam três novos registros de recursos (RRs): KEY, SIG e NXT. A RFC 2065 detalha o formato destes RRs e maiores detalhes do funcionamento da consulta de nomes de DNS podem ser obtido na RFC específica.

2.2.1 Distribuição de Chaves

"Um RRs KEY foi especificado permitindo ao DNS a distribuição de chaves públicas de criptografia incluindo campos com um identificador de algoritmo, além de uma série de indicadores, de entidade associada à chave ou a ausência de associação da chave" (RNP, 1998), sendo também anexadas à seção adicional de dados de forma automática sempre que possível.

2.2.2 Certificação da Origem e da Integridade dos Dados

Para garantia que a certificação ocorra será necessário obtenção por assinatura criptográfica associadas aos RRs, sendo que para cada RR de uma zona terá associado um RR SIG, ocasionando na maioria dos casos uma chave privada única que fica responsável por toda uma zona. "um resolvedor seguro aprendendo de modo confiável a chave pública da zona, pode verificar se os dados assinados são certificados é razoavelmente atuais." (RNP,1998)

> Esta chave de certificação da origem dos dados pertence à zona e não aos servidores que armazenam cópias dos dados. Isto significa que o comprometimento de um servidor, ou até mesmo de todos os servidores de uma zona, não necessariamente afeta o grau de garantia que um resolvedor tem de que ele pode determinar se o dado é legítimo. (RNP, 1998)

Outro particularidade é para a transmissão de RR SIGs assinando os RR das respostas não resolve, o problema para as respostas negativas, ou seja, a resposta dada por um servidor quando um nome ou o tipo procurado não existe. (RNP,1998)

Como forma de resolver esse problema foi introduzido o RR NXT (non-existent) ou não existente, que trás consigo a informação de que o nome que está sendo procurado não existe, o nome mais próximo imediatamente anterior e os tipo a ele associados. Conforme explicado em RNP (1998), "os RRs (NXT e SIG) deverão ser gerados a partir dos arquivos de zonas utilizados no DNS atual, usando uma chave privada guardada no servidor de nomes primário, não sendo gerados dinamicamente, o que não significam um acréscimo significativo de processamento para o servidor de nomes".

Existem dois casos em que um RR SIG não é assinado pela chave privada da zona.

2.2.2.1Primeiro caso da não assinatura

> Dá suporte à atualização dinâmica quando algumas estações têm permissão para atualizar dinamicamente (DNS dinâmico) dados de uma zona. A estação fica, então, responsável também pela assinatura dos RRs modificados. A chave pública desta estação estará presente no arquivo da zona e será assinada como os outros RRs da zona, mas os RRs atualizados/modificados devem ser assinados pela estação. (RNP, 1998)

2.2.2.2Segundo caso da não assinatura

> Suporta a certificação da transação e da requisição. A assinatura dos RRs não protege os cabeçalhos das mensagens do DNS nem suas requisições. Se os bits do cabeçalho foram falsificados por um servidor, existe pouca coisa que pode ser feita. Entretanto, é possível adicionar a certificação da transação. Tal certificação significa que um resolvedor pode ao menos ter certeza que ele está recebendo a resposta do servidor para quem ele acredita ter passado a consulta e que a mensagem não foi manipulada no caminho. Isto é feito adicionando, opcionalmente, um RR SIG no final de uma resposta que assina a concatenação da resposta do servidor com a consulta do resolvedor. (RNP, 1998)

Consultas também podem ser assinadas com um RR SIG no DNS atual podendo ser úteis futuramente nas requisições de atualização dinâmica ou consultas especiais. (RNP, 1998)

3 SEGURANÇA

3.1 Segurança em Redes de Computadores

A segurança de qualquer ambiente compartilhado por informações está relacionada à necessidade de proteção contra acessos não autorizados, manipulação dos dados armazenados na rede, assim como a sua integridade, e utilização não autorizada de computadores ou de seus respectivos dispositivos periféricos. Essa necessidade de proteção deve ser definida a partir das possíveis ameaças e riscos que a rede sofre. Dessa forma, procura-se evitar que pessoas não-autorizadas tenham acesso a informações particulares ou privilegiadas de qualquer usuário da rede. (THOMPSON, 2002)

Políticas de segurança e mecanismos aplicados a ambientes de comunicação de dados.

3.1.1 Política de Segurança

Política de segurança é definida como sendo um conjunto de leis, regras e práticas que dão as diretrizes de como uma instituição ou empresa protege e gerencia seus recursos e transmite os seus dados. Pode ser considerado seguro, um sistema de comunicação de dados que garante o cumprimento dessa política, devendo detalhar regras de como as informações e recursos oferecidos através da rede da organização devem ser manipulados.

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. (SOARES, 1995)

3.1.2 Mecanismos de Segurança

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)

Para implementação de uma política de segurança podemos utilizar vários mecanismos. Dentre alguns mecanismos importantes para segurança em redes de computadores são utilizados:

3.1.2.1Criptografia

Em meios de comunicação onde não é possível impedir que o fluxo de pacote de dados seja interceptado, podendo as informações ser lidas ou até modificadas, é necessária a criptografia. Nesse mecanismo, utiliza-se um método que modifique o texto original da mensagem transmitida, gerando um texto criptografado na origem, através de um processo de codificação definido por um método de criptografia. O pacote é então transmitido e, chegando ao destino, ocorre o processo inverso; isto é, o método de criptografia é aplicado agora para decodificar a mensagem, transformando-a na mensagem original.

Contudo, toda a vez que o método utilizado é descoberto, quebrando-se o código de criptografia, é necessário substituí-lo por outro diferente, o que acarreta no desenvolvimento de novos procedimentos para a implementação desse novo método, treinamento do pessoal envolvido, etc. Com o intuito de evitar tal problema, criou-se um novo mecanismo de criptografia, representado na figura 3.1 mostrada abaixo. Nesse novo modelo, um texto criptografado gerado a partir do texto normal varia de acordo com uma chave de codificação utilizada para o mesmo método de criptografia. Isto é, para uma mesma mensagem original e um mesmo método de criptografia, chaves diferentes produzem textos criptografados diferentes. Dessa forma, não adianta conhecer o método de criptografia para recuperar a mensagem original, porque, para recuperá-la corretamente, é necessário tanto o texto criptografado quanto a chave de decodificação utilizada. (THOMPSON, 2002)

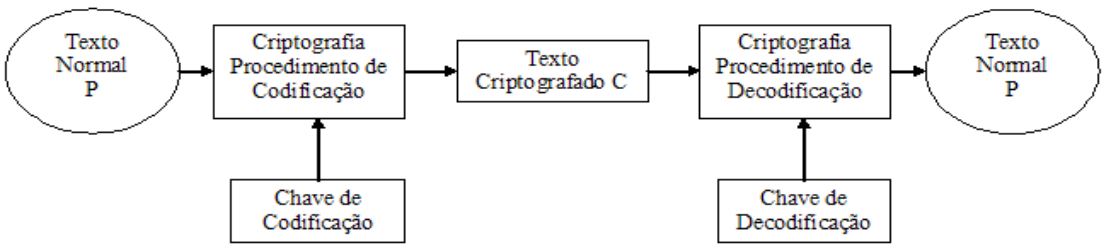


Figura 3.1: Método de criptografia utilizando chaves

3.1.2.2Integridade de dados

Os mecanismos para controle de integridade de dados estão presentes em dois níveis: controle da integridade de pacotes isolados e controle da integridade de uma conexão, ou seja, dos pacotes e da seqüência de transmissão.

No primeiro nível, existe a técnicas de detecção de modificações, que são normalmente associadas com a detecção de erros em bits, pacotes ou erros de seqüência introduzidos por enlaces e redes de comunicação, são usadas para garantir a integridade dos dados trafegados em uma rede. Entretanto, se os cabeçalhos dos pacotes de dados não forem devidamente protegidos contra possíveis modificações, pode contornar a verificação, desde que sejam conhecidas essas técnicas. Portanto, para garantir a integridade dos pacotes é necessário manter confidenciais e íntegras as informações de controle que são usadas na detecção de modificações.

Contudo controlar modificações na seqüência de pacotes transmitidos em uma conexão, exige técnicas que garantam a integridade desses pacotes, de forma a garantir que as informações de controle não sejam corrompidas, em conjunto com informações de controle de seqüência. Tais cuidados, apesar de não evitarem a modificação da cadeia de pacotes, garantem a detecção e notificação dos ataques. (COMER, 1998)

3.1.2.3Controle de acesso

Define quais as técnicas utilizadas pelo administrador do sistema para garantir o acesso limitado e restrito dos recursos da rede que cada usuário dispõe dentro da hierarquia.

Como técnicas podem destacar a utilização de listas ou matrizes de controles de acesso, que associam recursos a usuários autorizados; ou senhas e tokens associadas aos recursos, cuja posse determina os direitos de acesso do usuário que as possui.

Exemplo da utilização de tokens para controlar o acesso aos recursos de uma rede o método de controle de congestionamento de tráfego, onde, existem permissões, que são os tokens, que circulam pela rede. Sempre que um host deseja transmitir um novo pacote pela rede, ele primeiramente deve capturar uma dessas permissões e destruí-la, sendo que essa permissão destruída é regenerada pelo host que recebe o pacote no destino. Entretanto, esse método apresenta um problema: a distribuição das permissões depende das aplicações na rede e o próprio tráfego aleatório desses tokens causa um tráfego extra na rede, diminuindo assim o seu desempenho. A perda de uma permissão devido a uma falha qualquer na rede deve ser recuperada, de forma a evitar que a sua capacidade de transporte seja reduzida. a baixo representa a localização dos *root servers* e suas cópias espalhadas pelo mundo. (NORTHCUTT, 2001)

3.1.2.4Controle de roteamento

É o mecanismo responsável por garantir a transmissão de informação através de rotas fisicamente seguras, por canais de comunicação com níveis apropriados de proteção. Portanto, o administrador do sistema define as rotas preferenciais ou obrigatórias para a transferência dos dados que são garantidas pelo controle de roteamento dos pacotes. (THOMPSON, 2002)

3.2 Método de operação do atacante

A cada dia que passa novas formas de interferir e invadir computadores estão sendo colocadas em práticas, uma pessoa que tenha estudado um pouco de redes de

computadores consegue através da internet ter acesso a diversos ferramentas gratuitamente que podem ser utilizadas junto com algum conhecimento para se beneficiar de falhas em sistema ou descuido de usuários para provocar algum tipo de estrago. Uma grande preocupação dos administradores de sistema tem sido os ataques que as mesmas têm enfrentado não somente de tentativas de invasões externas, mas também internamente por indivíduos da própria organização. Em muitos países por significar até mesmo um risco à segurança nacional, os objetivos e métodos empregados nesses incidentes tem se tornado alvo de muitos estudos. (COMER, 2001)

A invasão de sistemas computacionais ocorre com finalidades diversas, podendo ser destacadas as seguintes:

• Obtenção de informações como roubos de segredos, números de cartões de crédito, senhas e outros dados relevantes ao intruso;

• Promover algum estrago em um site, destruição de informações e paralisação do sistema, por exemplo;

Conforme a habilidade e dependendo finalidade do invasor, a forma de operação pode sofrer algumas variações. Dessa forma, os passos tomados pelo atacante para comprometer um sistema computacional podem ser generalizados como segue:

• Definição do alvo do ataque;

• Identificar os pontos fracos e vulnerabilidades no sistema a ser atacado;

• Comprometimento inicial;

• Aumento do nível de permissão no sistema a ser atacado;

• Esconder rastros no sistema;

• Identificação do Sistema Operacional (SO) que será atacado;

• Encontrar formas de retornar ao SO;

• Apagar evidência de acesso antes de sair;

• Instalação de um backdoor para retorno ao SO; inventário e comprometimento de máquinas vizinhas.

Primeiramente o atacante escolhe de um alvo em potencial. Após começa a reunir informações sobre o sistema alvo a fim de identificar vulnerabilidades no sistema operacional ou serviços de rede disponíveis. Se o invasor ainda não possui uma combinação de usuário e senha válida para o sistema alvo, ele utiliza métodos como sniffing e adivinhação de senhas, engenharia social ou scanning para encontrar um ponto de entrada. (STALLINGS, 2005)

Uma vez encontrado um ponto de entrada o invasor realiza o comprometimento inicial do sistema. Essa primeira intrusão geralmente provoca muito “barulho”, especialmente se o sistema alvo estiver devidamente guarnecido, e costuma ocorrer quando ninguém está presente para “ouvir”. Tentativas de adivinhar senhas criam um número incomum de registros de logon falhos, comprometimentos de aplicativos através de *buffer overflow* geralmente ficam registrados nos arquivos de *log* ou geram mensagens de advertência que são produzidas em decorrência das várias tentativas de se tentar invadir o sistema. (STARLIN, 2001)

Depois que o atacante consegue acesso ao sistema, ele busca por privilégios irrestritos conta de administrador ou *root*. O invasor transfere programas maliciosos

para o sistema e tenta explorar vulnerabilidades que possam fornecer o acesso de *root*. Com acesso ilimitado, o atacante procura remover traços de sua presença, tornando-se "invisível", através da instalação de *rootkits* e *trojan horses*.

Quando o invasor obtém acesso de *root* e garante sua "invisibilidade", ele executa uma verdadeira varredura no sistema. O atacante procura saber o quanto sua presença perturba o sistema invadido e, por conseguinte, pode ser descoberto. Em seguida, ele investiga as medidas de segurança implementadas no sistema invadido, em alguns casos, o atacante até corrige vulnerabilidades existentes para impedir que outro invasor faça uso do sistema.

Após compreender as configurações do sistema, o atacante instala *backdoors* para facilitar seu retorno e apaga os rastros deixados por sua presença no sistema. Utilizando um *backdoor*, o invasor retorna de maneira mais discreta que o comprometimento inicial e faz um inventário acerca das informações existentes na máquina invadida e dos potenciais alvos da vizinhança, expondo toda a segurança de uma determinada organização. (NORTHCUTT, 2001)

4 UTILIZAÇÃO DO DNSSEC

4.1 Utilização do DNSSEC

O objetivo do DNSSEC é permitir que os servidores de DNS consigam autenticar as respostas das resoluções de nomes. Se um invasor conseguir falsificar um endereço IP para o site verdadeiro, o servidor de DNS, usando o DNSSEC, poderá verificar que aquela resposta não é a correta e assim saberá que deve descartá-la e tentar descobrir o real endereço do site novamente, até obter uma resposta válida.

A extensão DNSSEC criada pelo IETF (*Internet Engineering Task Force*) autentica as informações do DNS e garante que estas informações são autênticas e íntegras.

Sua utilização está crescendo a cada dia por ser um protocolo que agrega mais segurança a resolução de nomes, sendo possível garantir que os dados foram emitidos por quem se espera. Podemos verificar nos gráficos de registros mostrados abaixo.

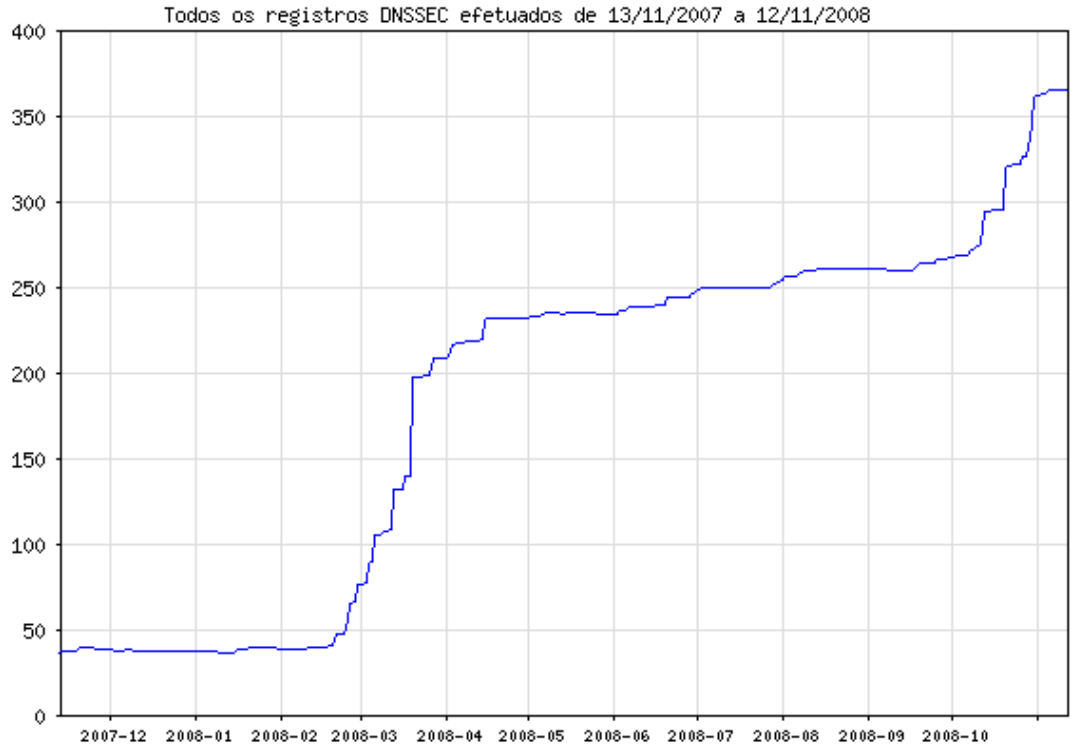


Figura 4.1: Crescimento da utilização do protocolo no último ano.

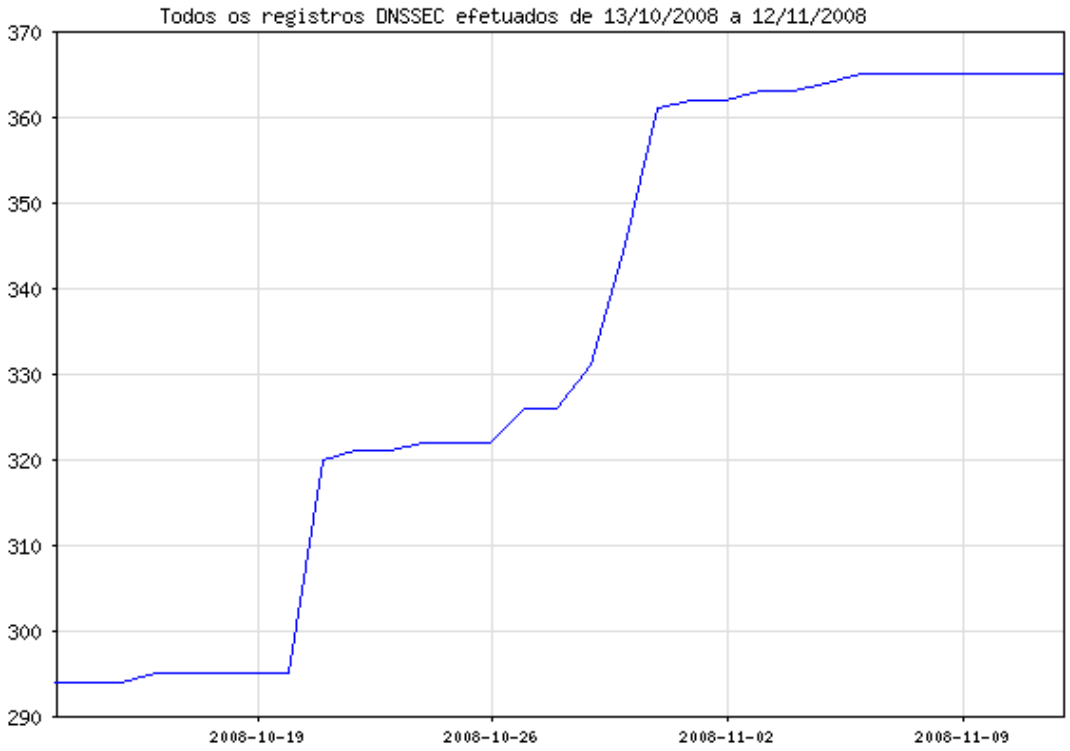


Figura 4.2: Crescimento da utilização do protocolo no último mês.

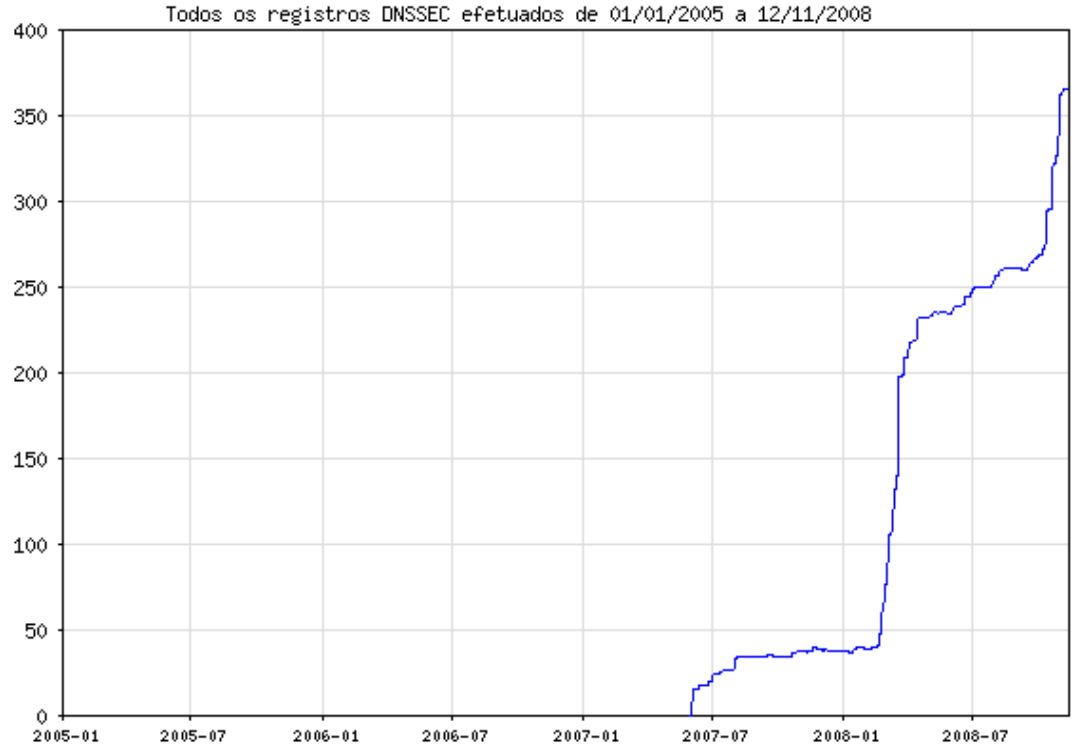


Figura 4.3: Crescimento da utilização do protocolo após surgimento no país.

A utilização obrigatória ainda está restrita aos que estiverem a baixos dos domínios JUS.BR e B.BR , mas diversos outros domínios já podem começar a utilização mesmo não sendo obrigatório.

Motivos para utilização, combater os ataques de envenenamento de cache, possibilidade de um novo serviço que poderia ser cobrado de determinado público, assegurar que seus dados estão chegando íntegros ao seu destino, possibilitar maior segurança para os usuários na internet, tratamento da assinatura de transferência de zona para servidores escravos quando sua implementação.

Gráfico de avanços do DNSSEC pelo mundo:

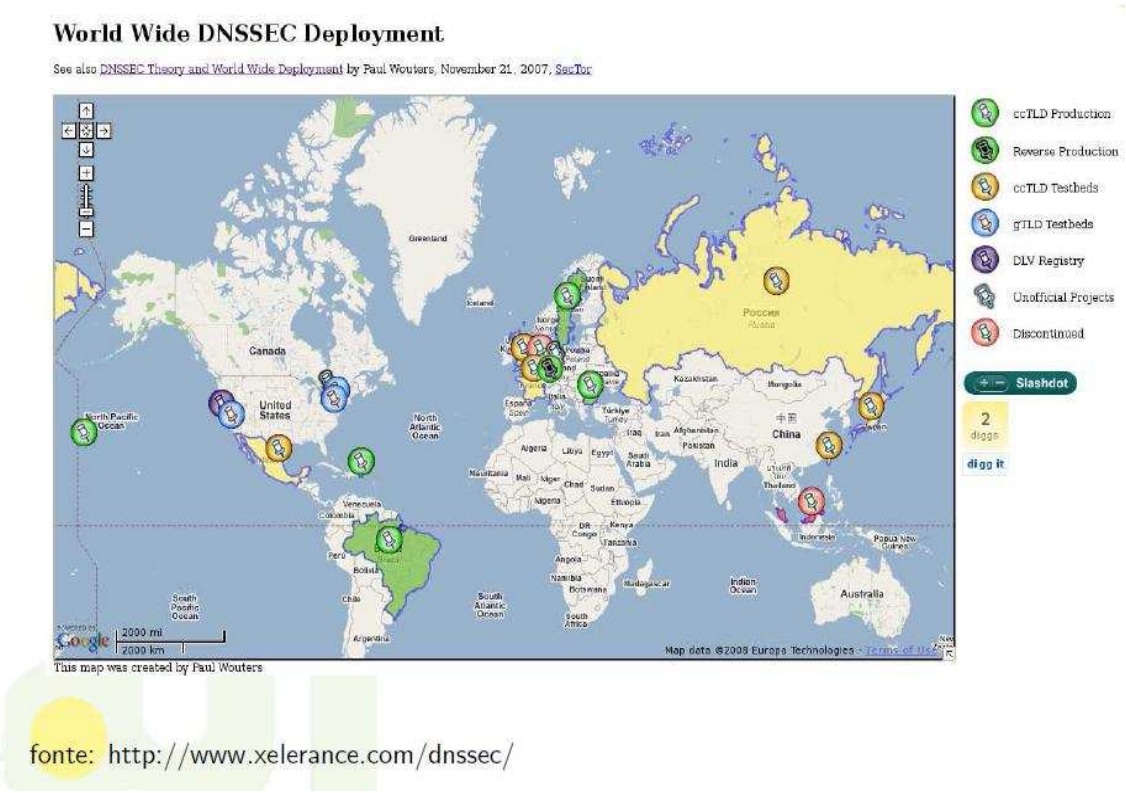


Figura 4.4: Utilização do DNSSEC pelo mundo

No Brasil os sites vinculados ao Poder Judiciário já estão utilizando o DNSSEC e os sites dos bancos vêm aderindo a essa nova tecnologia que faz essa implementação extra de segurança. (FOLHA ON-LINE, 2008)

No Brasil, alguns dos bancos ligados à FEBRABAN (Federação Brasileiras dos Bancos) que são os únicos que podem utilizar o B.BR já estão utilizando, destaque para Bradesco, Cooperativa Sicredi, Bonsucesso, Alfa, Banco do Paraná, Banrisul (Banco do Estado do Rio Grande do Sul) dentre outros. (FOLHA ON-LINE, 2008)

Todos esses avanços demonstram como o protocolo está sendo muito bem aceito pelas organizações que vêm iniciando a sua utilização. Neste momento com a migração dos bancos, mas certamente pelo início que foi no Poder Judiciário em todo o país.

4.2 Processo de aceitação

O objetivo desse trabalho é apenas demonstrar de forma simples um novo recurso disponível a partir da utilização e configuração do DNSSEC e não se deter a toda a sua configuração, vulnerabilidade, restrições ou as próximas etapas para continuação do protocolo, até porque sendo algo relativamente novo fica difícil de ser totalmente compreendido e principalmente o trabalho não contemplou a configuração na prática desse protocolo.

As contribuições a seguir são de implementação, configuração e roteiros que de configuração o que não dispensa a necessidade de estudados mais aprofundados para se colocar em prática esse protocolo. (DAVID, 2008)

4.2.1 Novo *Resource Records*

4.2.1.1DNSKEY Chave pública

É um resource record que armazena a chave pública da zona.

4.2.1.2RRSIG Assinatura do RRset

É um resource record que contém a assinatura de um RRset específico com uma determinada chave DNSKEY. (DAVID, 2008)

4.2.1.3DS Delegation Signer

É um hash do Record DNSKEY. Serve para informar que existe uma cadeia de confiança entre um domínio e seus subdomínios.

4.2.1.4NSEC

Aponta para o próximo nome e indica quais os tipos dos RRsets para o nome atual. Permite autenticar uma resposta negativa. (DAVID, 2008)

4.2.2 Roteiro – Configuração de um Servidor Autoritativo

Verificar a disponibilidade do domínio junto ao registro.br;

Instalar BIND;

Configurar um arquivo de zona no servidor Máster;

Configurar o arquivo named.conf no servidor Máster;

Configurar o arquivo named.conf no servidor Slave;

Executar o BIND (named) no servidor Máster;

Executar o BIND (named) no servidor Slave;

Registrar o domínio no Registro.br;

Aguardar nova publicação;

Realizar testes no servidor (DIG);

Criar chave KSK (dnssec-keygen);

Criar chave ZSK (dnssec-keygen);

Incluir as chaves geradas no arquivo de zona do servidor Máster;

Assinar a zona (dnssec-signzone);

Se existir delegações assinadas, incluir no arquivo de zona o DS de cada delegação e reassinar a mesma;

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

Atualizar o named.conf do servidor Slave habilitando DNSSEC-ENABLE;

Restartar o BIND (named) no servidor Máster;

Restartar o BIND (named) no servidor Slave;

Adicionar na interface de provisionamento o DS (localizado no arquivo dsset*);

Aguardar nova publicação. (DAVID, 2008)

4.2.3 Roteiro – Configuração de um Servidor Recursivo

Instalar biblioteca de desenvolvimento do OpenSSL;

Instalar BIND;

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

Configurar o arquivo named.conf habilitando DNSSEC-ENABLE e DNSSEC-VALIDATION;

Incluir a trusted-key no arquivo named.conf;

Executar o BIND. (DAVID, 2008)

4.2.4 Roteiro - Teste da Cadeia de Confiança

Instalar BIND com sigchase;

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

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

Realizar testes no servidor (DIG +sigchase). (DAVID, 2008)

5 CONCLUSÃO

Apesar da utilização de DNSSEC ser algo relativamente novo, vem sendo bem aceito pelo mercado, podendo ser comprovado pelos gráficos apresentado no decorrer do trabalho constatado o seu crescimento a cada dia, certamente o motivo de a certificação de nomes utilizando DNS ser altamente insegura tem contribuído para isso.

A tendência é pela migração inicial de todas as instituições financeiras ligadas a FEBRABAN passando a autenticar os seus domínios no novo B.BR até o final de 2009, e como os bancos historicamente são uma das entidades que mais investe em Tecnologia da Informação, principalmente para segurança de suas operações, a final estão lidando com bilhões ou trilhões em transações financeiras diariamente, a tendência é do mercado seguir o mesmo caminho assimilando que esse novo protocolo será a referência a ser utilizada para evitar a possibilidade de poluir ou adulterar o conteúdo dos caches dos servidores de nomes do DNS, e mesmo não sendo obrigatório sua utilização como no caso do JUS.BR e B.BR, será mais uma opção que contribui de forma significativa que está à disposição no mercado.

A RFC 2065 trata de detalhes bastante complexos das alterações propostas para esse protocolo, procurando validar os dados através de assinaturas criptográficas digitais. O trabalho teve apenas uma breve introdução ao uso do DNSSEC para resolver/atenuar o problema de segurança descrito e mostrar que com o uso de servidores de nomes seguros é possível garantir que os dados foram emitidos por quem se espera e não por alguém tentando invadir o seu sistema.

Associado a utilização de outros protocolos e soluções de segurança o DNSSEC será de grande contribuição para que seja reduzido o risco de um cliente ser enganado por um falsário que tenta se passar pelo sistema de um banco, por exemplo, com intuito de capturar informações privilegiadas.

Há muito ainda a ser feito, mas o primeiro passo já foi dado, então que seja na direção certa para que contribua com o emprego de tecnologias que venham a facilitar e nos ajudar cada vez mais nesse mundo globalizado em que vivemos.

REFERÊNCIAS

ALVESTRAND, H. T. et al. **Domain Name System Security Extensions**: RFC 2065. [S.l.]: Network Working Group, 1997. Disponível em: <http://www.ietf.org/rfc/rfc2065.txt>. Acesso em: 05 out. 2008.

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

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

DAVID, R. C. de C. et. al. **Tutorial DNSSEC**. Disponível em: <ftp://ftp.registro.br/pub/doc/tutorial-dnssec.pdf>. Acesso em: 16 set. 2008.

FALBRIARD, C. **Protocolos e Aplicações para Redes de Computadores**. São Paulo: Érica, 2002.

FURASTÉ, P. A. **Normas Técnicas para o Trabalho Científico**: explicitação das normas da ABNT. Porto Alegre: [s.n.], 2002. p. 49-56.

NORTHCUTT, S. **Segurança e Prevenção em Redes**. São Paulo: Berkeley, 2001.

FOLHA ON-LINE, Domínio "b.br" recebe adesão de dez bancos no Brasil. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u462296.shtml> Acesso em: 13 nov. 2008.

REGISTRO.BR, NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO. **Estatísticas de todos os domínios que utilizam DNSSEC para os gráficos dos registros efetuados**. Disponível em: <http://registro.br/stat/dnssec.html>. Acesso em: 12 nov. 2008.

RNP: Rede Nacional de Ensino e Pesquisa. **Boletim bimestral sobre tecnologia de redes de computadores.** 1998. Disponível em: <http://www.rnp.br/newsgen/9801/dnssec.html#ng-o>. Acesso em: 10 nov. 2008.

SOARES, L. F. G. **Redes de Computadores:** das LAN's, MAN's e WAN's às Redes ATM. Rio de janeiro: Campus, 1995.

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

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

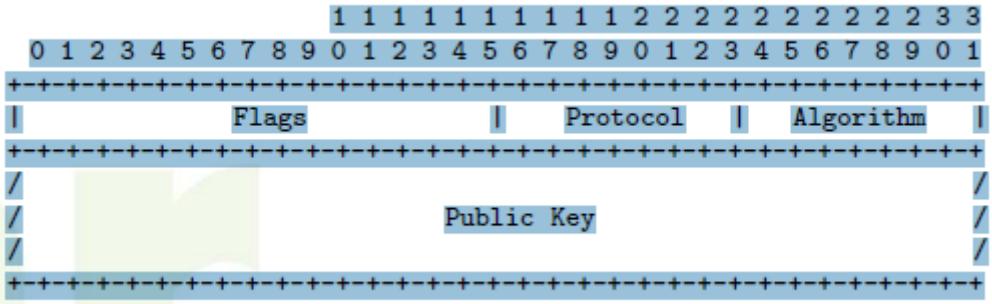
TANENBAUM, A. S. **Redes de Computadores**. 3.ed. Rio de Janeiro: Campus,
THOMPSON, M. A. **Proteção e Segurança na Internet**. São Paulo: Érica, 2002.

TÖPKE, C. R. **Provedor Internet:** arquitetura e protocolos. São Paulo: Makron Books, 2000.

WOUTERS, P. **World Wide DNSSEC Deployment**: utilização do DNSSEC pelo mundo. Disponível em: <http://xelerance.com/dnssec/>. Último acesso em: 15 nov. 2008.

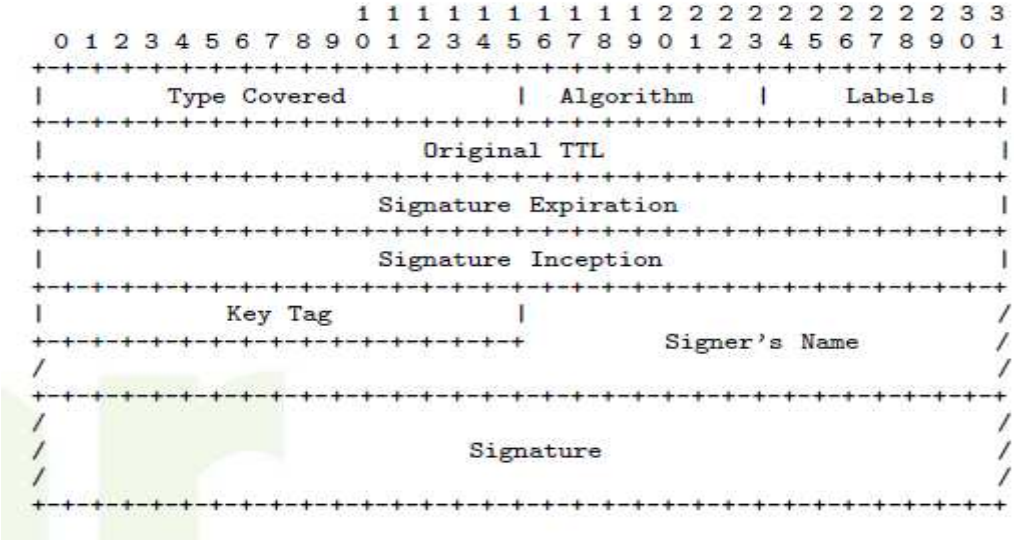
ANEXO A RR KEY

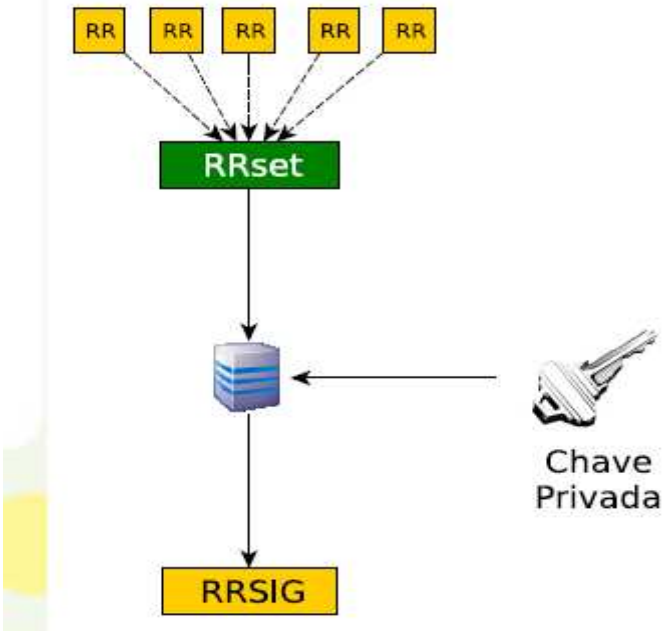
É um resource record que armazena a chave pública da zona.



ANEXO B RR SIG

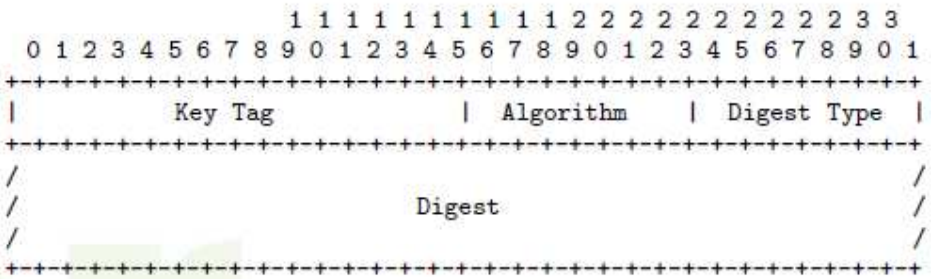
É um resource record que contém a assinatura de um RRset específico com uma determinada chave (RR KEY).

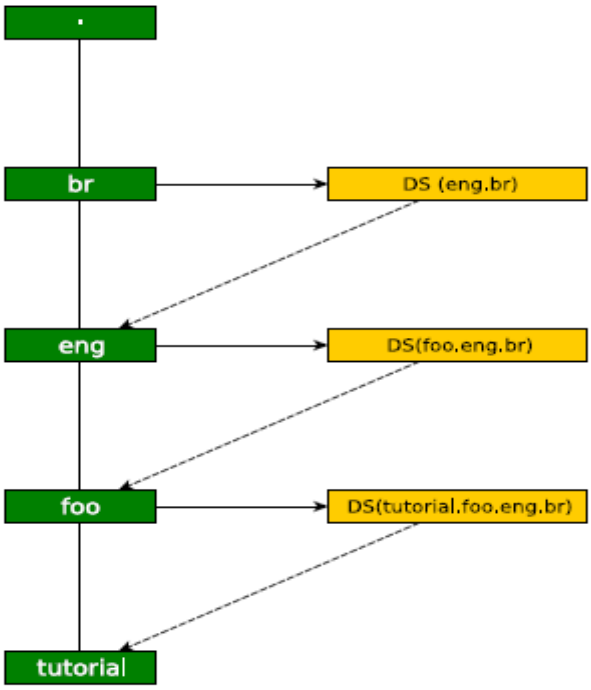




ANEXO C DS

É um hash do Record DNSKEY. Serve para informar que existe uma cadeia de confiança entre um domínio e seus subdomínios. Ponteiro para a cadeia de confiança, a qual garante a autenticidade das delegações de uma zona até um ponto de confiança.





ANEXO D RR NEXT

Aponta para o próximo nome e indica quais os tipos dos RRsets para o nome atual. Permite autenticar uma resposta negativa. Prova de não existência, com pré-assinatura, sem a necessidade de chaves on-line para assinatura on-demand. Diminuindo a possibilidade de DOS.