Everton Fernandes

Uma Análise do DNSSEC - Domain Name System Security Extensions

Florianópolis - SC, Brasil

Novembro de 2010

Everton Fernandes

Uma Análise do DNSSEC - Domain Name System Security Extensions

Monografia apresentada para obtenção do Grau de Bacharel em Sistemas de Informação pela Universidade Federal de Santa Catarina.

Orientador:
Msc. Darlan Vivian

Departamento de Informática e Estatística
Centro Tecnológico
Universidade Federal de Santa Catarina

Florianópolis - SC, Brasil

Novembro de 2010

Monografia de Projeto Final de Graduação sob o título *"Uma Análise do DNSSEC - Domain Name System Security Extensions"*, defendida por Everton Fernandes e aprovada em Novembro de 2010, em Florianópolis, Estado de Santa Catarina, pela banca examinadora constituída pelos senhores:

Msc. Darlan Vivian
Orientador

Prof. Dr. Ricardo Felipe Custódio
Professor Responsável

Msc. Martín Augusto Gagliotti Vigil
Universidade Federal de Santa Catarina

Dr. Roberto Samarone dos Santos Araújo
Universidade Federal do Pára

Msc. Juliano Romani
Universidade Federal de Santa Catarina

Dedicatória

Dedico este trabalho aos meus pais, meus avós e familiares que sempre estiveram presentes para me apoiar e incentivar.

Agradecimentos

Agradeço aos meus pais, Fernando e Jandira, e a minha irmã, Jéssica, por sempre estarem ao meu lado e depositaram grande confiança em mim. Agradeço também a minha namorada, Maria Izabel, pelo seu apoio e incentivo e ao meu orientador que me ajudou e me guiou para que este trabalho pudesse ser concluído, e ainda, aos amigos que me acompanharam durante todo o período da universidade.

Resumo

O *Domain Name System* - DNS é um dos principais serviços que suportam a Internet e responsável por converter os IPs em nomes e vice-versa. Como qualquer outro sistema computacional, o DNS possui falhas e vulnerabilidades que tendem a ser exploradas. Neste contexto, a proposta do *Domain Name System Security Extensions* - DNSSEC é adicionar algumas extensões de segurança ao serviço de resolução de nomes tornando-o mais seguro e confiável. Desta forma, o DNSSEC é uma alternativa para prover segurança entre as transações DNS utilizando como ferramentas as tecnologias de chaves assimétricas juntamente com as assinaturas digitais. Neste documento será transcrito uma fundamentação teórica a respeito do DNSSEC e seu funcionamento, bem como uma abordagem sobre a segurança de redes de computadores, mecanismos de segurança e os principais ataques existentes. Este trabalho também expõe uma breve comparação entre o funcionamento do DNS e do DNSSEC e uma reflexão a respeito do uso do DNSSEC em conjunto como protocolo SSL. Por último, é apresentado o relato da configuração e implementação do DNSSEC em um ambiente de produção.

Palavras-chave: DNS, DNSSEC, Criptografia, Segurança

Abstract

The *Domain Name System* - DNS is one of the main services that support the Internet and it's responsible for converting IPs addresses into names and vice versa. Like any other computer system, the DNS has vulnerabilities that may be explored by attackers. At this context, the proposal of *Domain Name System Security Extensions* - DNSSEC is to add some security extensions to the service name making it more secure and reliable. Using cryptography and asymmetric key technologies with digital signatures DNSSEC provide an alternative security arrangements between the DNS transactions.This document is a theoretical transcript about DNSSEC and how it works, as well as an approach to the security of computer networks, security mechanisms and the main existing attacks. This work also presents a brief comparison between the functioning of DNS and DNSSEC and a reflection on the use of DNSSEC together as SSL. Finally, this work presents a step-by-step guide to assist users to install the DNSSEC.

Keywords: DNS, DNSSEC, Cryptography, Security

Sumário

Lista de Figuras

Lista de Siglas

ARPANET	Advanced Research Projects Agency Network
ccTLD	Country Code Top Level Domains
DIG	Domain Information Groper
DNS	Domain Name System
DoS	Denial of Service
DDoS	Distribuited Denial of Service
FTP	File Transfer Protocol
gTLD	Generic Top Level Domains
HSM	Hardware Security Module
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
KSK	Key Signing Key
LACNIC	Latin American and Caribbean Internet Addresses Registry
NIR	National Internet Register
RIR	Regional Internet Register
RFC	Request for Comments
SSL	Secure Sockets Layer
TLD	Top Level Domain
TTL	Time to Live
ZSK	Zone Signing Key

1 Introdução

No início de sua existência, as redes que interligavam computadores eram usadas principalmente para fins acadêmicos, militares ou por funcionários de organizações que compartilhavam documentos, troca de mensagens eletrônicas, dispositivos de impressão e outros recursos. Neste cenário restrito a segurança não era o foco principal. Atualmente, com o crescimento das redes, milhões de usuários realizam operações bancárias, operações de comércio eletrônico e acesso remoto à informações sigilosas e a segurança das redes se tornou uma preocupação diária de nível prioritário dentro de qualquer organização.[1]

Desde a década de 70 as redes vêm crescendo e aumentando cada vez mais sua complexidade. Com a popularização da Internet nos últimos anos foi necessário criar e manter infraestruturas e serviços que possam acolher um número cada vez maior de usuários. Um destes serviços é o DNS (Domain Name Service), que foi criado a partir da necessidade de traduzir números IP, grandes e complicados, para algo que pudesse ser facilmente lembrado por pessoas comuns.

Fundamentalmente as redes de computadores são inseguras, todavia existem diversas soluções para se implementar segurança em uma rede. Pode-se escolher dentre várias opções, desde ações implementadas no nível da camada física até o nível da camada de transporte. Existem inúmeras possibilidades de tecnologias para garantir a segurança das redes desde protocolos na camada de enlace até *firewalls* e *gateways* seguros.[2]

Uma das técnicas mais utilizadas para manter o sigilo das informações enviadas através de uma rede de dados é o uso da criptografia, ou seja, as informações são embaralhadas de tal maneira que só computadores autorizados consigam resgatar a informação original.[3]

Com o advento de novas tecnologias surgem novos problemas. A segurança de rede tem preocupado muitos profissionais nos últimos anos e os servidores DNS são alvos constante de ataques. Em 1995, no estado de Utah, Paul Vixie escreveu um artigo intitulado "DNS and BIND Security Issues"abordando os problemas do DNS e do BIND.

Para solucionar alguns dos problemas do DNS foi proposto um padrão internacional,

estendendo a tecnologia DNS já existente, cujo nome chamou-se DNSSEC (Domain Name System Security Extensions). Este novo sistema garante uma resolução de nomes mais segura, reduzindo o risco de manipulação de dados e informações, e para isso utiliza um mecanismo baseado na tecnologia de criptografia de chaves públicas.

1.1 Motivação

Com o constante avanço da tecnologia e a descoberta de problemas e falhas, a utilização de ferramentas e mecanismos que possam garantir a segurança das redes e de sistema se torna inevitável. É necessário obter o conhecimento de todos os artifícios que existem e que se julga ser necessário para garantir a segurança da informação.

A motivação para esse trabalho de conclusão de curso é realizar uma pesquisa sobre os protocolos DNS e DNSSEC, bem como uma revisão nos mecânismo de segurança existentes que auxiliam na resolução segura de nomes em uma rede de computadores.

1.2 Objetivo Geral

O objetivo deste projeto é pesquisar sobre o protocolo DNSSEC para construir uma base referencial de pesquisa fazendo uma análise a respeito da necessidade dessas novas extensões de segurança.

1.3 Objetivos Específicos

- Realizar um levantamento bibliográfico sobre o assunto;
- Estudo dos principais documentos de referência (RFC);
- Demonstrar as diferenças básicas entre o DNS e o DNSSEC e a necessidade de sua utilização;
- Apresentar as principais extensões do DNSSEC e suas características;
- Entender a necessidade do uso das extensões de segurança do DNS e o que ocasionou essa necessidade.
- Apresentar uma revisão da área de Segurança, mecanismos existentes e métodos de ataque ao DNS.

- Mostrar quais são os principais passos necessários para a instalação e utilização do DNSSEC em uma rede de computadores.
- Demonstração prática da configuração de um ambiente de rede para utilizar o DNSSEC relatando as etapas executadas e os dados obtidos.

1.4 Delimitação do Escopo

A proposta deste trabalho é pesquisar o protocolo DNS e seu sucessor reunindo as informações necessárias para um conhecimento aprofundado do DNSSEC e seu funcionamento. A proposta ainda abrange uma revisão sobre os mecanismos de segurança existentes e uma análise comparativa entre o DNS e suas extensões de segurança.

1.5 Organização do Trabalho

O presente documento abordará o DNSSEC provendo uma base teórica para sua compreensão e entendimento da necessidade de sua utilização no ambiente de rede de computadores. O entendimento se dará pela revisão bibliográfica do assunto e das RFC referentes, e sempre que necessário, buscando auxílio através de figuras, tabelas, exemplos e esquemas.

A seguir será demonstrado a maneira de organização deste documento e as informações encontradas em cada uma das seções. A estrutura organizacional do trabalho consiste em:

- Capítulo 1: Introdução

  Abordagens iniciais sobre o assunto e apresentação do trabalho.

- Capítulo 2: Fundamentação Teórica

  Capítulo de fundamental importância para o bom compreendimento do trabalho e da eficácia do DNSSEC. São apresentados os principais conceitos sobre criptografia e seu funcionamento.

- Capítulo 3: DNS

  Neste capítulo é apresentado desde o histórico até o funcionamento básico do DNS e todos os mecanismos que utiliza para executar a resolução dos nomes.

- Capítulo 4: DNSSEC

  Nesta seção são abordados os principais conceitos a respeito do DNSSEC como a distribuição das chaves, origem e integridade dos dados, garantia de não existência, processo de autenticação e a forma canônica.

- Capítulo 5: Segurança

  Aborda os principais mecanismos de segurança e os principais tipos de ataques a redes de computadores encontrados na literatura.

- Capítulo 6 : Funcionamento do DNS e do DNSSEC

  Esta seção expõe o funcionamento básico de uma requisição DNS e DNSSEC finalizando com uma comparação entre elas. Também é abordado sobre a utilização do DNSSEC ou do SSL.

- Capítulo 7 : Configuração do DNSSEC

  Apresenta as etapas executadas em laboratório para a configuração do DNSSEC com exposição dos dados.

- Capítulo 8 : Conclusão

  Conclusão sobre o trabalho desenvolvido e a utilização do DNSSEC.

- Apêndice A: Roteiro de Instalação

  Um roteiro básico de instalação, utilização e teste para o funcionamento do DNSSEC em servidores autoritativos e recursivos.

2 *Fundamentação Teórica*

2.1 Introdução

Este capítulo tem como objetivo explanar a cerca dos conhecimentos básicos a respeito das tecnologias utilizadas pelo DNSSEC para garantir a integridade dos dados. Para tal, será apresentado uma breve revisão bibliográfica contendo a fundamentação e concepções básicas de criptografia para situar o leitor sobre as considerações básicas e de fundamental importância para a compreensão dos capítulos futuros.

2.2 Conceitos de Criptografia

Criptografia é a ciência e arte, ligadas a Matemática, de escrever mensagens em forma de código e faz parte de um campo de estudos que trata das comunicações secretas.

Sua origem remete as palavras gregas *kryptós*, "escondido"e *gráphia*, "escrita"e sua aplicação utiliza técnicas pelas quais a informação pode ser transformada da sua forma original para uma forma ilegível, impossibilitando sua leitura por indivíduos não autorizados.

De acordo com Stallings [4], a criptografia pode ser definida como a área de estudo onde uma mensagem passa por um processo de codificação chamado cifragem, tendo como resultado dessa operação uma mensagem cifrada. E o processo inverso, ou seja, recuperar a mensagem original a partir de uma mensagem cifrada é chamado de decifragem.

Os algorítmos atuais de Criptografia são basicamente divididos em algorítmos simétricos e assimétricos, e as técnicas empregadas visam garantir cinco requisitos básicos:

- Sigilo;
- Integridade;

- Autenticidade;
- Não Repúdio;
- Tempestividade.

2.3 Resumo Criptográfico (Função *Hash*)

Uma função *hash* é uma função matemática que calcula uma representação condensada de uma mensagem ou arquivo. Ela recebe uma cadeia de bits de comprimento qualquer e retorna uma outra cadeia de bits de comprimento fixo, chamado de resumo.[5]

O resumo (as vezes também chamado de impressão digital da mensagem) serve como uma imagem representativa compacta da mensagem, e pode ser usada como se fosse unicamente identificável com os dados de entrada. O *hash* é usado em conjunto com a criptografia assimétrica e é utilizado para garantir a integridade de um documento digital. Algumas de suas propriedades são:

- Deve ser computacionalmente inviável fazer a operação inversa, ou seja, dado um resumo criptográfico, deve ser muito difícil obter a mensagem original;
- Duas mensagens semelhantes, não iguais, devem produzir um resumo completamente diferente;
- Deve ser computacionalmente fácil e rápido produzir o resumo criptográfico.

2.4 Criptografia Simétrica

A criptografia simétrica utiliza a mesma chave para cifrar e decifrar uma mensagem. Isso significa que a chave deve ser de conhecimento tanto do emissor quanto do receptor da mensagem. Normalmente na criptografia simétrica, o algorítmo para cifrar e decifrar é basicamente o mesmo, mudando apenas a forma como é utilizada a chave. Devido a esta técnica de criptografia ser muito utilizada ao longo dos anos e por seus algoritmos serem normalmente muito simples, muitos aperfeiçoamentos e avanços foram realizados neste tipo de sistema criptográfico. [6]

A criptografia simétrica gira em torno do compartilhamento de uma chave. Tanto o indivíduo remetente da mensagem, quanto o indivíduo destinatário possuem a chave. E

é neste compartilhamento que consiste o grande entrave no uso da criptografia simétrica, pois se a chave for compartilhada em um canal não seguro, nada impede que um indivíduo malicioso faça a interceptação desta chave e tenha acesso a mensagem original.

O remetente da mensagem, de posse da chave, aplica um algorítmo de cifragem simétrica sobre a mensagem que deseja enviar.O resultado desta operação é um texto embaralhado e ilegível que será enviado ao destinatário.

O indivíduo destinatário possui uma cópia da chave e o conhecimento do algoritmo que foi utilizado e desta maneira pode executar o processo inverso, tendo acesso a mensagem original. A figura abaixo ilustra o uso do algorítmo simétrico e o compartilhamento da chave.

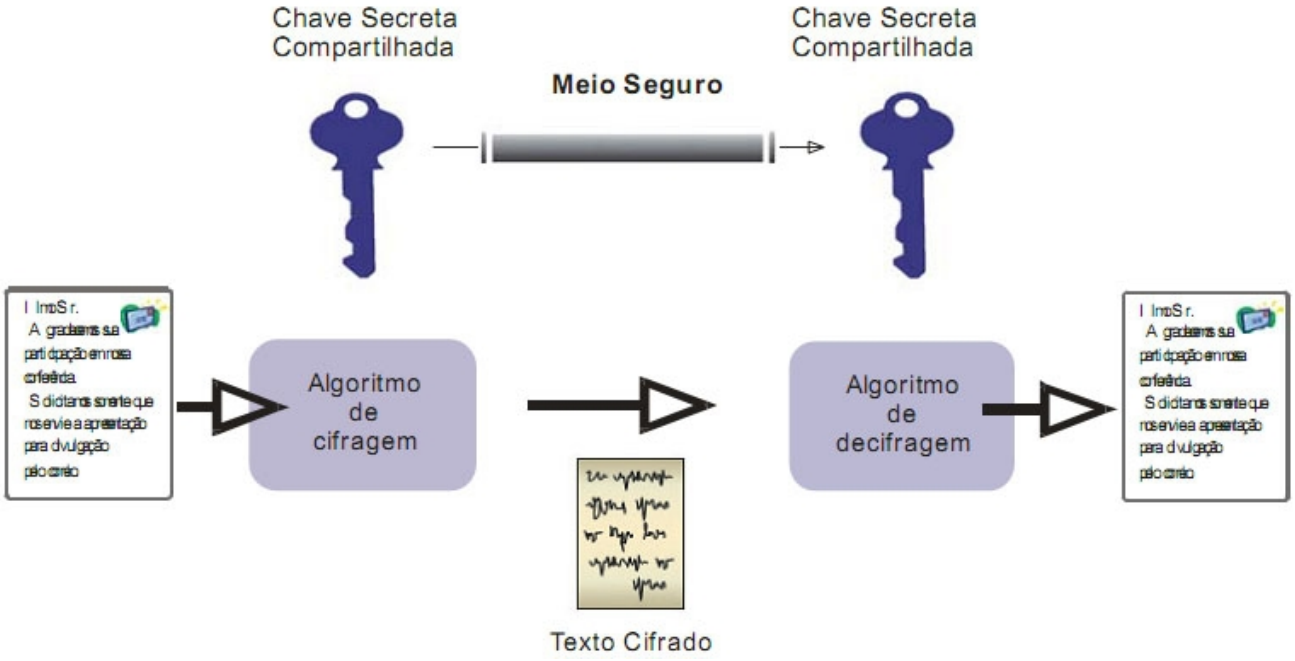

Figura 1: Criptografia Simétrica - retirado de [7]

2.5 Criptografia Assimétrica

Criptografia assimétrica, ou também chamada, criptografia de chaves públicas é um modelo que utiliza um par de chaves: a chave privada e a chave pública. Se por um lado a chave pública é distribuída livremente, pelo outro a chave privada deve ser conhecida somente pelo seu dono. [4]

Este modelo de chaves públicas foi publicado por Diffie e Hellman [8] em 1976. Cerca

de um ano depois Ron L. Rivest, Adi Shamir e Leonard M. Adleman publicaram o primeiro algorítmo que utilizava o modelo de chaves públicas denominado RSA (iniciais dos sobrenomes Rivest, Shamir, Adleman). Mais recentemente, no ano de 2002, Hellman sugeriu que o algorítmo fosse chamado de Diffie-Hellman-Merkle em reconhecimento as contribuições de Ralph Merkle para a criptografia de chaves públicas. A figura abaixo esquematiza a cifragem de uma mensagem com uma chave privada.

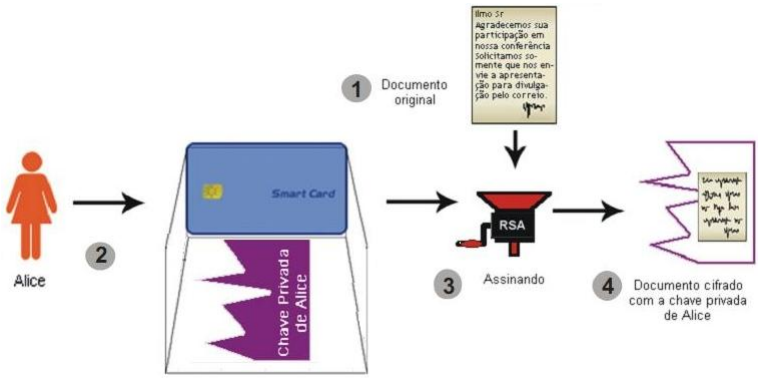

Figura 2: Cifragem com chave privada - retirado de [7]

Em um algorítmo de criptografia assimétrica a mensagem a ser enviada é cifrada com a chave pública do destinatário e poderá ser decifrada somente pela chave privada homóloga. Do mesmo modo, uma mensagem cifrada com a chave privada poderá ser decifrada somente pela chave pública correspondente.

Com a utilização do modelo de chaves públicas o problema do compartilhamento da chave é reduzido. Entretanto, devido as suas caracterísiscas, a criptografia assimétrica acaba por gerar um custo computacional maior na execução de suas funções. A figura abaixo esquematiza a decifragem de uma mensagem utilizando a chave pública.

2.6 Conclusão

Com a revisão e estudo dos conceitos básicos, fica evidenciado a importância da criptografia para a segurança na resolução de nomes sendo estes a base para as extensões de segurança do DNS. No próximo capítulo será dado ínicio às abordagens referentes ao DNS, seu funcionamento e sua necessidade.

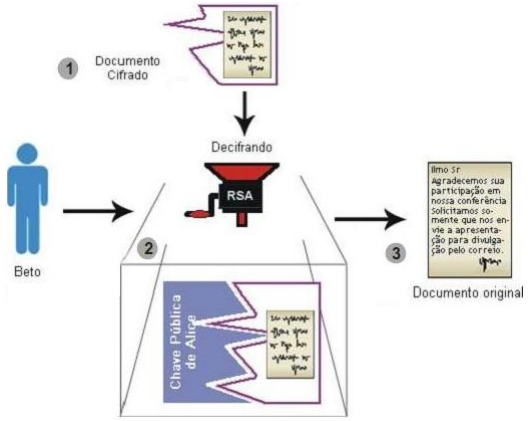

Figura 3: Cifragem com chave pública - retirado de [7]

3 DNS

3.1 Introdução

Este capítulo tem como objetivo primordial a apresentação do protocolo DNS descrevendo um pequeno histórico sobre sua criação e utilização, sua estrutura básica e seu funcionamento.

No ínicio dos anos 70, na rede de computadores do Departamento de Defesa Norte-Americano (ARPANET) existia apenas um arquivo, HOSTS.TXT, que continha as informações do mapeamento de endereços IP para nomes. Esse arquivo era mantido e atualizado em um único servidor central e sempre que uma estação cliente optasse por obter um mapeamento atualizado dos nomes e IP era necessário realizar o carregamento do arquivo.

Para uma rede com algumas centenas de computadores essa estratégia funcionava razoavelmente bem. Entretanto, ao acoplar milhares de estações e servidores à rede, essa abordagem se torna impraticável. Além do arquivo de *hosts* se tornar muito grande, seria necessário uma gerência centralizada de nomes para evitar conflitos, o que seria algo totalmente fora de cogitação para uma rede mundial.

Para resolver esse tipo de problema era necessário um Sistema de Nomes de Domínios. No ano de 1983 Paul Mockapetris descreveu o serviço DNS nas RFC 882 e 883, mais tarde reformuladas pelas RFC 1034 e 1035. A primeira implementação do DNS foi executada pela Universidade da Califórnia - Berkeley. Um ano mais tarde essa implementação daria origem a o que hoje é conhecido como servidor de domínios, o BIND (Berkeley Internet Name Domain).

Para se ter acesso a um web site ou para realizar o envio de um e-mail, é necessário ao sistema cliente saber em qual dos servidores espalhados pela rede se encontra hospedada a página ou o e-mail. Estas informações sobre a localização dos dados encontram-se armazenadas em servidores DNS.

O protocolo DNS é um sistema que realiza o mapeamento de endereços IP para nomes de domínios 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 bancos de dados distribuídos para implementar esse esquema de nomenclatura. Ele é usado principalmente para mapear os *hosts* e destinos de mensagens de correio eletrônico em endereços IP.[1]

Como garantia, um domínio pode definir vários servidores DNS, sendo sempre o servidor primário o primeiro a ser consultado na tentativa de resolução de nome. Caso o primário venha a falhar ou estar indisponível, o próximo servidor de consulta é acionado. Este servidor é chamado de secundário e é uma espécie de cópia de segurança do servidor DNS primário. No caso de uma falha no servidor secundário o próximo servidor será consultado e assim sucessivamente até que se obtenha a resposta solicitada.[9]

3.2 Árvore DNS e o Espaço de Nomes

Toda a estrutura de banco de dados do sistema de gerenciamento de nomes e domínios está organizada de forma hierárquica e distribuída na Internet. Este tipo de organização permite uma fácil administração e torna o tamanho do banco ilimitado e escalonável.

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 "exemplo.dns.com"será quebrado e resolvido começando por *com*, depois *dns* e finalmente *exemplo* - itens chamados respectivamente *top-level domain*, *second-level domain* e *third-level domain*. É nessa ordem que o endereço IP para "exemplo.dns.com"será obtido.[10]

A estrutura hierárquica encontrada no sistema de gerenciamento de nomes e domínios segue uma topologia em árvore. Esta topologia é composta por um elemento principal chamado de raiz que possui ligações para os outros elementos, denominados galhos ou filhos. Estes elementos podem se ligar a outros galhos e assim sucessivamente. Um elemento que não possui galho é conhecido como folha ou nó terminal. Um servidor DNS localizado no primeiro nível da hierarquia é chamado de servidor raiz. Na figura 4 pode-se observar um exemplo de hierarquia utilizada pelo DNS.

Existem dois tipos de domínios de nível superior: genéricos e de países. Os domínios genéricos originais eram *com* (comercial), *edu* (instituições educacionais), *gov* (instituições governamentais), *int* (organizações internacionais), *mil* (órgãos das forças armadas), *net* (provedores de rede) e *org* (organizações sem fins lucrativos). Os domínios de países

incluem uma entrada para cada país, conforme a definição da ISO 3166.[1]

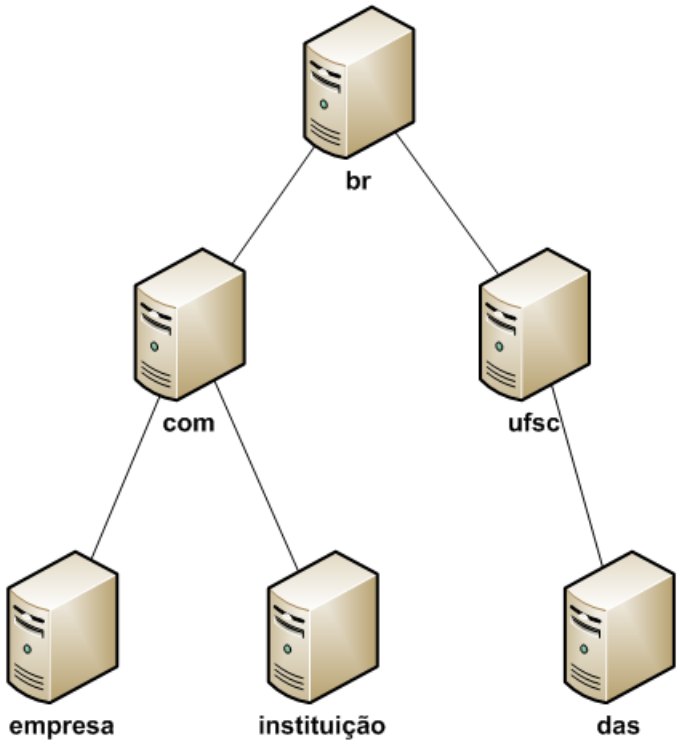

Figura 4: Topologia em árvore do DNS

3.3 Servidor Raiz

Os servidores raizes espalhados pela Internet iniciam o nível hierárquico do sistema DNS. Estes servidores não resolvem diretamente as requisições de resolução DNS, ao invés disso, eles encaminham a requisição a outros servidores autoritativos que respodem a requisição ou a repassam para o próximo nível hierárquico.

Também conhecidos como *root servers*, possuem uma tabela que indica qual DNS é o responsável pela resolução de cada extensão de domínio (na sigla em inglês, TLD - *Top Level Domain*). Estas extensões podem ser de dois tipos:

- gTLD (na sigla em inglês, *Generic Top Level Domains*) - são os chamados domínios genéricos que são utilizados no mundo todo.
- ccTLD (na sigla em inglês, *Country Code Top Level Domains*) - são as extensões referentes a cada país e são administradas pelos mesmos.

Ao todo existem treze servidores DNS raiz espalhados pelo globo. Estes servidores são conhecidos como *root servers*, e destes trezes, dez estão localizados fisicamente nos Estados Unidos, um na Ásia e dois na Europa. Algumas réplicas desses servidores estão espalhadas por todo o mundo, inclusive no Brasil, para ajudar a aumentar a base instalada. Ficou convencionado que cada servidor seria representado por uma letra do alfabeto (Servidor A, Servidor B, e assim por diante) e estes servidores podem ser replicados em diversos lugares do mundo para que o tempo de consulta tenha latência menor em relação à uma consulta no servidor original.[11]

A figura abaixo mostra a localização dos trezes servidores raízes (nomeados de A à M) e de suas réplicas espalhadas pelo globo. Este mapa está disponível e pode ser melhor explorado em *http://root-servers.org/*.

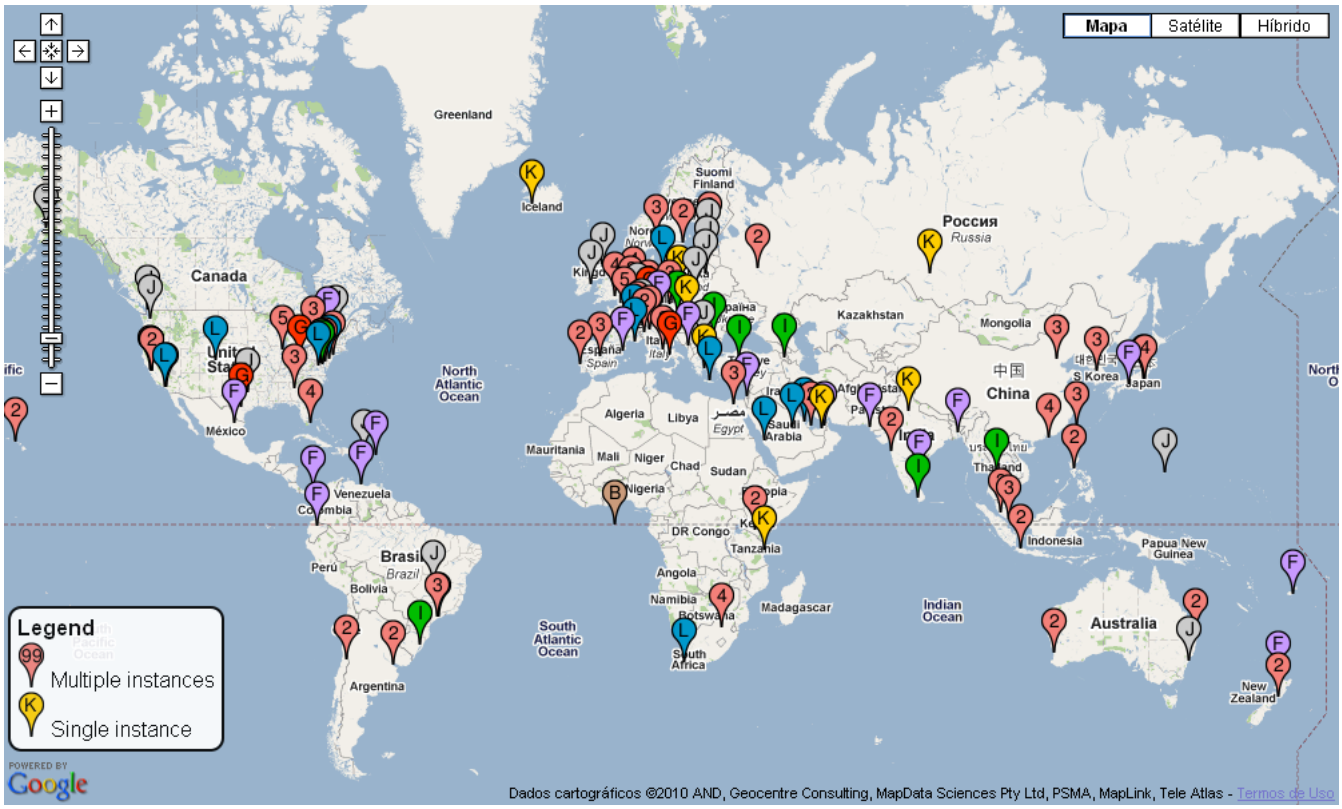

Figura 5: Servidores Raízes e suas réplicas espalhados pelo mundo.

Os servidores raízes acabam não tendo um grande volume de consulta, porque os provedores de acesso e as empresas de comunicação ao redor do globo arquivam no cachê de seus servidores a tabela dos *root-servers*. Estas referências podem ficar guardadas por um período de tempo para evitar um acesso externo tornando necessário uma nova consulta ao servidor raiz quando uma nova TLD é criada.

3.4 Servidores Autoritativos

É dito um servidor autoritativo aquele que, possui autoridade sobre um determinado domínio e pode responder às requisições DNS sobre este, informando que o mesmo possui os arquivos de zonas com os registros dos recursos solicitados. Para que um servidor possa responder por um domínio é necessário uma concessão pelos registros de domínios oficiais de acordo com a região. No Brasil, quem fornece a concessão para que um servidor possa responder por um domínio é a entidade denominada Registro.br (*http://www.registro.br/*).

A entidade Registro.br tem sua autoridade reconhecida pelos *root-servers*, pois é um NIR (na sigla em inglês, *National Internet Register*) responsável pelo Brasil e é autorizado pelo LACNIC (na sigla em inglês, *Latin American and Caribbean Internet Addresses Registry*) que é um dos cinco RIR (na sigla em inglês, *Regional Internet Register*) que existem espalhados pelo mundo.

3.5 Servidores Recursivos

É considerado um servidor recursivo aquele que, ao receber uma solicitação e não dispondo da informação em seu cachê ou não sendo o próprio domínio, realiza consultas recursivas em outros servidores, até obter uma resposta válida, sendo esta positiva ou negativa.

3.6 Registro de Recursos

Em um banco de dados DNS encontram-se um ou mais arquivos de zona. Cada zona contém um conjunto de recursos estruturados responsáveis por infomar qual o tipo de mapeamento será feito para um determinado domínio.

Segundo as RFC (do inglês, *Request For Common*) 882, 1035, 1183, 2065 e 2181 e 2535 existem alguns registros de recursos essenciais para que um sistema de nomes de domínio seja eficiente.

Abaixo estão citados os registros mais importantes e suas funções.

Básicos:

- A - Mapeamento de nome para endereço (IPv4);

- AAAA - Mapeamento de nome para endereço (IPv6);
- PRT - Resolução reversa (endereço-nome);
- MX - Controla o encaminhamento de e-mail.

Zonas:

- SOA - Define uma zona DNS;
- NS - Identifica servidores de zonas, delega subdomínios.

Segurança (Providos pelo DNSSEC):

- KEY - Chave pública para um nome DNS;
- SIG - Zona autenticada, com assinatura;
- NSEC - Garante a não existência de um registro;
- DS - Cadeia de segurança na delegação de zonas.

Opcionais:

- CNAME - Apelidos ou nomes alternativos.

3.7 Conclusão

Com os temas relacionados neste capítulo, fica claro a fundamental importância do protocolo DNS para a arquitetura atual da Internet. Fica evidenciado, também, sua estrutura escalável e sua falta de segurança no que se refere a integridade e autenticidade dos dados da resposta uma vez que, a utilização de qualquer mecanismo que possa garatir segurança não está presente no protocolo.

Neste cenário, surge a necesssidade de extensões de segurança e com isso as implementações do protocolo DNSSEC. No capítulo a seguir são abordados os recursos e mecanismos utilizados pelo DNSSEC para a garantia de uma resolução de nomes confiável.

4 DNSSEC

4.1 Introdução

Como todo software, sistema computacional ou serviço de rede, o DNS está suscetível a erros e falhas de segurança. O DNSSEC é uma extensão do DNS, ou seja, é um complemento às funções já existentes no DNS tornado-as mais seguras e oferecendo maior confiabilidade aos usuários na Internet.

Esta foi razão primordial para a criação do DNSSEC: oferecer um serviço de resolução de nomes onde é possível garantir e verificar que as respostas obtidas são íntegras, autênticas e confiáveis. Para tal, o DNSSEC provê alguns novos registros que serão abordados nas próximas seções.

A partir de agora será dada a abordagem sobre o trabalho realizado, focando na importância que a segurança das extensões oferecidas pelo DNSSEC podem adicionar ao sistema de resolução de nomes tornando-o mais seguro e confiável.

Segundo Evi Nemeth, Garth Snyder e Trent R. Hein .[12], o DNSSEC é um conjunto de extensões 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 obtendo suas respectivas respostas.

- Estes dados DNS realmente provêm do proprietário da zona?
- Estes são realmente os dados enviados pelo proprietário?

Para implementar essas funcionalidades, o DNSSEC faz uso da criptografia de chave pública e introduz um novo conjunto de registros com funções específicas: assinar outros registros (RRSIG), divulgar a chave pública que valida as assinaturas digitais de um determinado domínio (DNSKEY), garantir a não existência de outros registros (NSEC) e garantir a continuidade do "canal de segurança"na delegação de zonas (DS). [13]

4.2 As Chaves e Sua Distribuição

A utilização de chaves públicas e privadas pelo DNSSEC (herdado do conceito de assinatura digital) implica na distribuição das chaves públicas aos usuários que desejam validar as informações recebidas. O DNSSEC prevê duas diferentes maneiras para resolver esse impace:

- Enviar a chave para cada um dos clientes que deseja validar seus dados;
- Adicionar um *hash* da chave pública na zona imediatamente acima da sua.

A primeira solução proposta visa enviar a chave de forma segura aos clientes, utilizando por exemplo emails assinados, servidores FTP autenticados, SSL, entre outros. Entretanto, esta abordagem é inviável do ponto de vista de atualização das chaves, pois cada cliente precisaria estar atento as atualizações de chave para requisitar uma nova cópia.

A segunda maneira utiliza algo semelhante ao processo de delegação de zonas (dados distribuídos com apontadores para os próximos servidores da hierarquia) adaptado as necessidades do DNSSEC na forma do registro DS (abordado em uma seção a seguir).

As chave públicas e privadas possuem uma validade. Este período em que a chave é válida quase sempre é apresentado no formato "não antes"e "não depois". este fato é relevante, pois quanto mais informações criptografadas com uma chave um possível atacante possuir acesso, mais possibilidades surgirão para um atacante tentar quebrar o algorítmo. Dessa maneira, faz-se necessário a troca e a divulgação das chaves com alguma frequência. Ou seja, quanto maior a frequência da troca das chaves, maior será o trabalho para atualizar todas as suas cópias. Neste cenário uma chave com um uso menor se mostraria mais interessante para distruibuir aos clientes. Dessa necessidade surge a chave KSK.

Esta chave é utilizada para apenas para assinar os registros DNSKEY. Como a KSK assina poucos registros, pode-se definir uma validade maior para ela (e pedir para que os clientes a troquem com menos frequência)

Já a outra chave, a ZSK assina todos os outros registros da zona, precisará ser trocada numa frequência maior, porém com um impacto menor aos clientes (não é necessário nenhuma mudança na configuração do servidor).

Um registro chamado KEY foi especificado permitindo ao DNS a distribuição de chaves públicas de criptografia incluindo campos com um identificador de algorítmo, além de uma série de indicadores, de entidade associada à chave ou a ausência de associação da chave.[14]

Este registro KEY é anexado automaticamente pelos servidores de DNS à seção de dados adicionais, sempre que for possível. Este registro que contém um campo com o identificador do algorítmo de criptografia da chave pública, informações necessárias ao uso da chave pública, e também algumas informações como tipo da entidade associada a chave, entre outros.

4.2.1 Registro KEY

O registro abaixo contém uma chave de zona DNS para o endereço "exemplo.com".

```
exemplo.com. 86400 IN DNSKEY 256 3 5 ( AQPSKmynfzW4kyBv015MUG2DeIQ3Cbl+BBZH4b/0PY1kxkmvHjcZc8no
                                       kfzj31GajIQKY+5CptLr3buXA10hWqTkF7H6RfoRqXQeogmMHfpftf6z
                                       Mv1LyBUgia7za6ZEzOJBOztyvhjL742iU/TpPSEDhm2SNKLijfUppn1U
                                       aNvv4w== )
```

Figura 6: Exemplo de um registro KEY

Os primeiros quatros campos de textos indicam o nome do proprietário, TTL (*Time to Live* - quanto tempo será armazenado em cachê), classe e o tipo do registro (DNSKEY). O valor "256"indica que a chave de zona tem valor 1 no campo de flag. O valor "3"é fixo e de uso interno do protocolo. O valor "5"indica o algorítmo da chave pública . O resto dos caracteres são a chave pública codificada em Base64.

4.3 Certificação da Origem e da Integridade dos Dados

Para garantir que a certificação ocorra será necessário a obtenção da assinatura associada aos registros (para cada registro de uma zona será associado um registro RRSIG) que na maioria dos casos foi gerada a partir de uma chave privada única que fica responsável por toda uma zona. "Um resolvedor seguro conhecendo de modo confiável a chave pública da zona, pode verificar se os dados assinados são certificados e razoavelmente atuais."[14]

Esta chave 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.[14]

O DNSSEC usa a criptografia de chaves públicas para assinar e autenticar conjuntos de registros. As assinaturas digitais são armazenadas no registro RRSIG e são utilizadas para autenticação conforme descrito na RFC-4035 [15]. Um cliente pode usar esse registro RRSIG para autenticar conjuntos de registros de uma zona. Este registro RRSIG deve ser utilizado somente para carregar material de verificação (assinatura digital) usado para garantir as operações DNS.

Quando um cliente (geralmente um servidor recursivo) recebe a resposta de uma consulta DNSSEC, ele recebe duas informações: o conjunto de registros consultado e o registro RRSIG. No processo de verificação o cliente calcula o *hash* do conjunto de registro recebido, usa a chave pública da zona para decifrar o registro RRSIG e faz comparação entre o *hash* gerado e o obtido na decifragem. Caso sejam iguais, então a resposta é válida; caso contrário os dados foram alterados e a resposta é do tipo *SERVFAIL*. [13]

Na prática, o registro RRSIG contém a assinatura para um conjunto de registros com o nome, classe, tipo e também especifica um intervalo de validade. Ele usa o algorítmo, o nome do signatário e o identificador da chave para identificar o registro que contém a chave pública que o validador pode usar para verificar a assinatura digital.

Como cada conjunto de registros autoritativos de uma zona precisa ser protegido por uma assinatura digital, o registro RRSIG deve estar presente para nomes que contenham um registro CNAME. Esta é uma das mudanças na especificação tradicional do DNS, que afirma que se um CNAME está presente para um nome, este será o único tipo permitido naquele nome. Um registro RRSIG e um registro NSEC devem existir para o mesmo nome, bem como um registro CNAME em uma zona assinada.

Existe também um registro auxiliar chamado SIG RDATA que contém algumas informações tais como o tipo de conjunto de registro que é assegurado pelo registro RRSIG, o algorítmo utilizado, dados sobre o nome do proprietários, dados auxiliares para a validação da assinatura digital e TTL do conjunto de registros.

O RRSIG também contém dados sobre a data de início e vencimento. Esses campos definem um prazo de validade para a assinatura e o registro não deve ser usado para autenticação da assinatura fora desse intervalo de validade.

Em um registro RRSIG, o valor do campo "Nome do Signatário"identifica o dono da chave, pode ser usado por um validador para autenticar a assinatura e deve conter o nome da zona do conjunto de registros cobertos pela assinatura. Um remetente não deve usar a compactação de nome DNS no campo "Nome do Signatário"quando transmitir um

registro RRSIG.

A assinatura em si, fica armazenada no campo "Assinatura"e cobre o RRSIG, RDATA, o conjunto de registros especificados pelo nome do proprietário, e o tipo de cobertura. O formato desse campo depende do tipo de algorítmo usado na assinatura e o conjunto de registros é utilizado na forma canônica (vide seção Forma Canônica e a Ordem dos Registros).

4.3.1 Registro RRSIG

O registro abaixo armazena a assinatura para o conjunto de registros do endereço "host.exemplo.com"

```
host.examplo.com. 86400 IN RRSIG A 5 3 86400 20030322173103 ( 20030220173103 2642 examplo.com.
                    oJB1W6WNGv+ldvQ3WDG0MQkg5IEhjRip8WTrPYGv07h108dUKGMeDPKijVCHX3DDKdfb+v6o
                    B9wfuh3DTJXUAfI/M0zmO/zz8bW0Rznl8O3tGNazPwQKkRN20XPXV6nwwfoXmJQbsLNrLfkG
                    J5D6fwFm8nN+6pBzeDQfsS3Ap3o= )
```

Figura 7: Exemplo de um registro RRSIG

Os primeiros quatros campos de textos indicam o nome do proprietário, TTL (*Time to Live* - quanto tempo será armazenado em cachê), classe e o tipo do registro (RRSIG). O valor "A"representa o tipo de cobertura, o valor "5"indica o algorítmo utilizado para criar a assinatura. O valor "3"é número de *labels* do nome do proprietário. O valor "86400"é TTL original do tipo "A". Os valores "20030322173103"e "20030220173103"são a data inicial e final da validade da assinatura. O valor "2642"é o identificador da chave e "exemplo.com"é o nome do proprietário. Os outros caracteres são a assinatura codificada em Base64.

4.4 Garantia de Não Existência

Este registro mantém as informações sobre o próximo nome na zona. A grosso modo, cada registro mantém uma referência, através do NSEC, para o próximo registro. Sua função é apontar de forma canônica e consecutiva o próximo conjunto de registros de uma zona e assim criar uma cadeia de confiança. Dessa maneira, um cliente pode utilizar um registro NSEC autenticado para dizer que determinardo conjunto de registros não estão presentes em uma zona durante uma consulta.

O registro NSEC é uma resposta autenticada da não existência de um domínio e fornece informações sobre dois aspectos: a indicação do próximo nome seguro e o tipo

de conjunto de registros existentes, como pode ser observado mais detalhadamente na RFC-3845 [16].

Em uma zona, o último registro NSEC aponta para o primeiro registro encontrado na zona. Por consequência, se uma consulta buscar por um nome não existente na zona, um regisro RRSIG que abrange todo o NSEC se mostrará presente na resposta, autenticando a não existência do nome de domínio ou do tipo de dados solicitado. [17]

Como cada nome autoritativo de uma zona precisa ser parte de uma cadeia NSEC, o registro NSEC deve estar presente para nomes que possuem o registro CNAME. Esta é uma diferença da especificação tradicional do DNS que afirma que se um CNAME está presente para um nome, ele é o único tipo permitido para este. Um registro RRSIG e um registro NSEC devem existir para um mesmo nome assim como um registro CNAME em uma zona assinada.

A figura abaixo demonstra como funciona a assinatura dos registros NSEC exemplificando o processo de garantia de não existência.

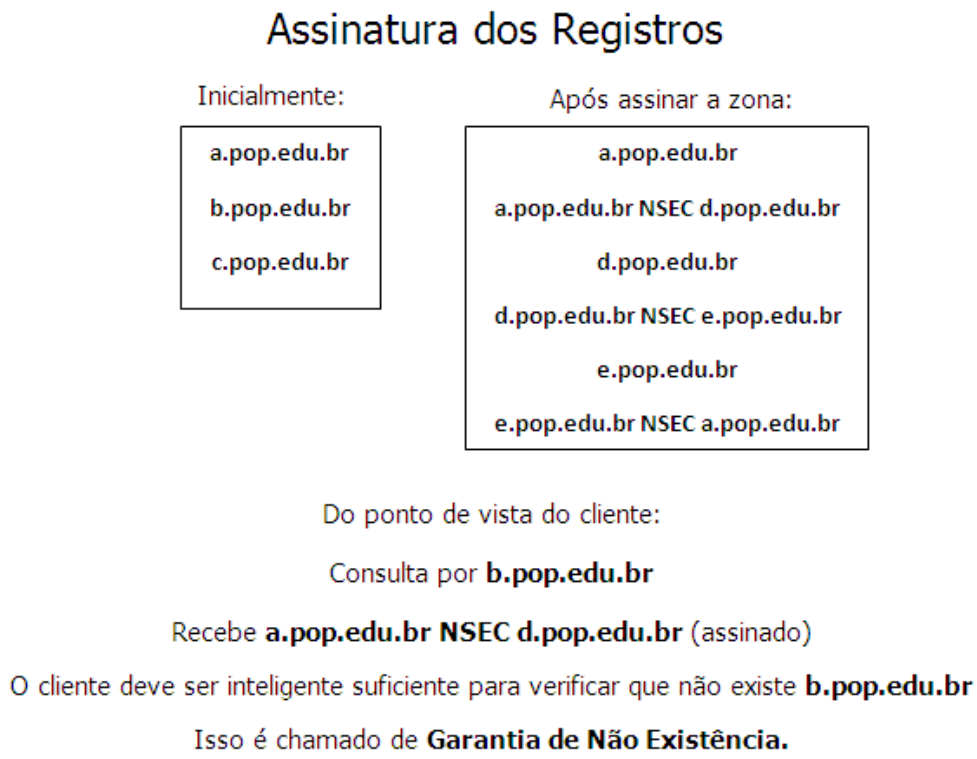

Figura 8: Esquema assinatura de registros

No registro NSEC existe um campo "Próximo Nome de Domínio"que contém o próximo domínio seguro, na ordem canônica da zona, com dados autoritativos ou contém um ponto de delegação NSEC. O valor do campo do último registro NSEC da zona aponta

para o nome da zona que está no topo. Isso indica que o nome do dono do registro NSEC é o último nome, na ordem canônica, da zona. Para mais informações sobre ordem canônica, consulte a seção "Forma Canônica e a Ordem dos Registros".

Um remetente não deve usar a compactação DNS no campo "Nome do Signatário"quando transmitir um registro RRSIG.

No registro NSEC, existe um campo que identifica o tipo do conjunto de registros existentes no registro NSEC do dono e é separado em 256 blocos. Cada bloco tem pelo menos um tipo ativo de registro e é codificado utilizando um octeto simples (0 a 255) de bits. Os valores desses bits identificam os tipos, bit 1 corresponde ao tipo 257, se for o bit 2 corresponde ao tipo 258 e assim por diante.[18]

4.4.1 Registro NSEC

O exemplo abaixo do registro NSEC identifica um conjunto de registros associados a "a.exemplo.com"identificando o próximo domínio seguro.

```
a.exemplo.com. 86400 IN NSEC b.exemplo.com. ( A MX RRSIG NSEC TYPE1234 )
```

Figura 9: Exemplo de um registro NSEC.

Os primeiros quatro campos indicam o nome do proprietário, TTL (*Time to Live* - quanto tempo será armazenado em cache), classe e o tipo do registro (NSEC). O valor "b.exemplo.com"é o próximo domínio seguro da ordem canônica. Os valores "A", "MX", "RRSIG", "NSEC"e "TYPE123"indicam que esses registros estão associados ao domínio "a.exemplo.com"

4.5 O processo de Autenticação

A idéia é armazenar um *hash* da chave de uma zona em sua zona pai e deixar a tarefa de ancorar a chave diretamente no cliente (servidor recursivo) somente quando não houve a possibilidade de fazer isso com a zona pai. Ou seja, se todos os domínios aplicarem esse processo, é necessário apenas ancorar as chaves da zona raiz no cliente. [13]

Os registros DS armazenados no pai apontam para as zonas filhas de forma sucessiva. Essa cadeia de confiança é responsável por prover a autenticidade das delegações de uma zona até um ponto de confiança. O ponto de confiança é onde há uma chave pública

confiável fornecida pela empresa responsável por admnistrar os domínios de primeiro nível. No Brasil o registro.br fornece uma *trusted key* para a zona ".br".

Para criar uma cadeia de confiança, faz-se necessário a criação de um registro DS na zona filha e então a adição deste DS à zona pai. A figura abaixo exemplifica esta idéia:

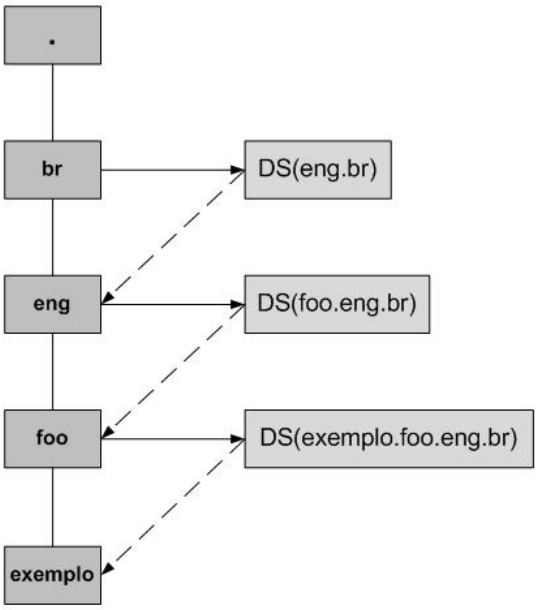

Figura 10: Cadeia de confiança.

O registro DS faz referência a um registro KEY e é utilizado no processo de autenticação. Ele se refere a chave armazenando o código da chave, o algorítmo e o resumo criptográfico da chave. Somente o resumo da chave já bastaria para identificar a chave pública, contudo o código da chave e o algorítmo ajudam a tornar o processo de identificação mais eficiente.[18]

O código da chave é usado para ajudar a selecionar a chave, porém esse codigo não identifica unicamente uma chave. É possível que duas chaves distintas tenham o mesmo nome de proprietário, mesmo tipo de algoritmo e o mesmo código. Uma implementação que utiliza somente o código da chave para selecionar uma chave pode, em algumas circunstâncias, selecionar erroneamente a chave.

Autenticando o registro DS, um resolvedor pode autenticar a chave cujo DS se refere. O processo de autenticação é detalhadamente descrito na RFC-4035 [15].

O registro DS e sua chave correspondente tem o mesmo nome do proprietário mas são armazenados em diferentes locais. O registro DS é encontrado somente no lado superior (pai) de uma delegação e é autoritativo. Por exemplo, o registro DS para "exemplo.com"é armazenado na zona *com* (zona pai) em vez da zona *exemplo.com* (zona filha). Esta

abordagem simplifica o gerenciamento e assinatura das zonas DNS.

Existe um campo chamado DS RDATA que contém os dados referentes ao código da chave, o algoritmo, o tipo de resumo criptográfico e o conteúdo do resumo. Para o código da chave é reservado um campo com 2 octetos, 1 octeto para o algorítmo, 1 octeto para o tipo de resumo. O tamanho do campo do resumo pode variar de acordo com o algorítmo de *hash* utilizado.

O registro DS faz a ligação da cadeia de autenticação através das zonas e por isso este registro requer um cuidado extra no processamento. O registro KEY, referenciado pelo registro DS, deve ser uma chave de uma zona DNSSEC. Entretanto, se a chave não for referente a uma zona DNSSEC o registro DS não deve ser utilizado no processo de validação.

4.5.1 Registro DS

O exemplo abaixo demonstra um registro DS e seu registro DNSKEY correspondente.

```
example.com. 86400 IN DNSKEY 256 3 5 ( AQOeiiR0GOMYkDshWoSKz9XzfwJr1AYtsmx3TGkJaNXVbfi/
                                       2pHm822aJ5iI9BMzNXxeYCmZDRD99WYwYqUSdjMmmAphXdvx
                                       egXd/M5+X7OrzKBaMbCVdFLU Uh6DhweJBjEVv5f2wwjM9Xzc
                                       nOf+EPbtG9DMBmADjFDc2w/r ljwvFw== ) ;

example.com. 86400 IN DS 60485 5 1 ( 2BB183AF5F22588179A53B0A98631FAD1A292118 )
```

Figura 11: Exemplo de um registro DS.

Os primeiros quatro campos indicam o nome do proprietário, TTL (*Time to Live* - quanto tempo será armazenado em cachê), classe e o tipo do registro (DS). O valor "60485"é o código da chave referente a "exemplo.com", o valor "5"identifica o algorítmo utilizado pela chave e o valor "1"identifica o algorítmo utilizado para criar o resumo criptográfico. O último campo contém o resumo codificado em Base64.

4.6 Forma Canônica e a Ordem dos Registros

A ordenação canônica dos nomes é necessária para construir a cadeia de nomes NSEC. A forma canônica dos registros e a ordenação dentro de um conjunto de registros também são necessárias para construir e verificar registros RRSIG.[18]

Para o propósito de segurança do DNS, o nome dos proprietários são ordenados pelo tratamento individual das partes dos nomes levando em consideração a justificação a

esquerda.

Para executar a ordenação canônica de um conjunto de nomes DNS o primeiro passo é a classificação de acordo com a sua parte mais significativa. Para nomes em que a parte mais importante é idêntica é necessário continuar classificando com a próxima parte mais significativa e assim por diante até chegar ao final do nome.

No exemplo abaixo os nomes estão ordenados de forma canônica. A parte mais significativa é "exemplo". Assim "exemplo"é ordenado primeiramente, seguido por todos os nomes terminados por "a.exemplo"e então pelos terminados por "z.exemplo". Em cada um dos níveis os nomes são ordenados da mesma maneira.

```
example
a.example
yljkjljk.a.example
Z.a.example
zABC.a.EXAMPLE
z.example
\001.z.example
*.z.example
\200.z.example
```

Figura 12: Exemplo de ordenação canônica.

Para que a ordenação canônica possa ser executada e assim atender aos requisitos de segurança do DNS, é necessário que a forma canônica dos registros sigam alguns padrões:

- Cada nome de domínio no registro deve estar totalmente expandido (sem compressão) e qualificado;
- Todas as letras maiúsculas (US-ASCII) no nome do proprietário do registro devem ser substituídas pelas letras minúsculas (US-ASCII) correspondentes.
- Se o tipo do registro for NS, MD, MF, CNAME, SOA, MB, MG, MR, PTR, HINFO, MINFO, MX,RP, AFSDB, RT, SIG, PX, NXT, NAPTR, KX, SRV, DNAME, A6, RRSIG ou NSEC, todas as letras maiúsculas (US-ASCII) nos nomes DNS contido no registro RDATA devem ser substituídas pelas letras minúsculas (US-ASCII) correspondentes.
- Se o nome do proprietário de um registro for uma máscara ele deve estar em seu formato original não expandido, incluindo o caracter "*"(sem substituição do coringa);
- O TTL (*Time to Live*) do registro é definido para seu valor original como aparece na zona autoritativa ou no campo Original TTL do registro RRSIG.

Para um conjunto de registros não é permitido registros duplicados (múltiplos registros com o mesmo nome de proprietário, classe, tipo e registro RDATA). Portanto, quando uma aplicação identifica registros duplicados ao colocar o conjunto de registros na forma canônica, é necessário tratar este fato como um protocolo de erro.[19]

4.7 Conclusão

O DNSSEC ameniza alguns dos problemas encontrados na atual tecnologia DNS. Falsas informações DNS criam oportunidades para o roubo de informações de terceiros ou alterações de dados em diversos tipos de transações. No protocolo DNS, um ataque onde a informação corrompida é extremamente difícil de ser detectado e, na prática, impossível de ser prevenido. [13]

De acordo com o que foi abordado neste capítulo, as práticas e métodos utilizados pelo DNSSEC garantem a confiabilidade dos dados recebidos. Com a ajuda dos registros KEY e RRSIG é possível garantir de autênticidade e integridade das informações providas. Já com o auxílio do NSEC fica evidente a não existência de um registro e o registro DS cria uma cadeia de confiança entre as zonas.

Assim, o DNSSEC suaviza alguns dos fatores de risco encontrados em uma rede de computadores. Serão abordados, no próximo capítulo, alguns dos principais ataques que podem ocorrer a computadores conectados a uma rede. O enfoque se dará sobre as ofensivas direcionadas especificamente ao DNS bem como tecnologias e mecanismos existentes para a proteção contra esses ataques.

5 Segurança

5.1 Introdução à Segurança em Redes de Computador

Segurança é um assunto abrangente e inclui inúmeros tipos de problemas. Em sua forma mais simples, a segurança se preocupa em garantir que pessoas mal-intencionadas não leiam ou, pior ainda, modifiquem secretamente mensagens enviadas a outros destinatários. Outra preocupação da segurança são as pessoas que tentam ter acesso a serviços remotos que elas não estão autorizadas a usar. Ela também lida com meios para saber se uma mensagem supostamente verdadeira é um trote. A segurança trata de situações em que mensagens legítimas são capturadas e reproduzidas, além de lidar com pessoas que tentam negar o fato de terem enviado determinadas mensagens.[1]

A segurança de ambientes com informações compartilhadas está relacionada à necessidade de proteção contra acessos não autorizados, manipulação, a integridade e a utilização não autoriza dos dados ou de recursos disponíveis. Essa necessidade de proteção deve ser definida a partir das possíveis ameaças e riscos que a rede sofre. Dessa maneira, procura-se evitar que pessoas não autorizadas tenham acesso a informações particulares ou privilegiadas de usuários da rede.

A grande maioria dos problemas relacionados à segurança é causada intencionalmente por indivíduos maliciosos que tentam obter algum benefício, chamar atenção ou prejudicar alguém. Tornar uma rede segura envolve muito mais que simplesmente mantê-la livre de erros de programação e de implementação.

Os problemas de segurança das redes podem ser divididos nas seguintes áreas interligadas: sigilo, autenticação, não repúdio e controle de integridade. O sigilo está relacionado com a manutenção das informações longe de usuários não autorizados. Em geral, a autenticação cuida do processo de determinar com quem você está se comunicando antes de revelar informações sigilosas ou entrar em uma transação comercial. O não repúdio trata de assinaturas e como provar que seu cliente realmente efetuou uma transação. Por fim,

como você pode se certificar de que uma mensagem recebida é realmente legítima e não algo que um indivíduo mal-intencionado modificou ou criou?[1]

No mundo real, normalmente as pessoas conseguem distinguir um documento original de uma fotocópia. Pessoas são autenticadas por outras ao terem seus rostos, vozes ou caligrafia reconhecidas. As comprovações de assinatura são feitas através de assinaturas em papel timbrado, de símbolos em alto relevo, entre outras. Nenhuma dessas opções está disponível eletronicamente mas existem outras soluções para a resolução destes impasses.

Este capítulo tem como objetivo explanar os principais conceitos de segurança em redes de computadores. Abordando desde o uso de políticas de segurança, mecanismos de segurança mais comuns existentes e algumas formas de ataques a computadores conectados à rede, sempre com o foco voltado ao DNS, as próximas seções visam o esclarecimento da necessidade da utilização do protocolo DNSSEC.

5.2 Políticas de Segurança

Segundo a RFC-2196 [20], uma política de segurança é um conjunto formal de normas internas padronizadas pela organização que devem ser seguidas à risca por todos os utilizadores dos recursos da rede para que todas as possíveis ameaças sejam minimizadas e combatidas eficientemente pela equipe de segurança.

Uma política de segurança tem como propósito informar aos usuários, equipe de segurança e gerentes, os seus deveres e obrigações para a proteção da tecnologia e do acesso à informação. A política deve especificar os mecanismos através dos quais estes requisitos podem ser alcançados. Outro propósito para a política é servir como ponto de referência para que se possa adquirir, configurar e auditar sistemas computacionais e de redes, que sejam adequados aos requisitos propostos. Assim sendo, uma tentativa de utilizar um conjunto de ferramentas de segurança na ausência de pelo menos uma política de segurança implícita não faz sentido.

A política de segurança pode ter como uma de suas partes uma política de uso apropriado (do inglês *Appropriate* - ou *Acceptable* - *Use Policy* - AUP). Esta política de uso indica o que os usuários devem e não devem fazer em relação aos diversos componentes do sistema ou rede, incluindo o tipo de tráfego permitido. A AUP deve ser tão explícita quanto o possível evitando ambiguidades ou más interpretações

Toda a documentação que define a política de segurança da organização deve deixar

de fora os aspectos técnicos relativo a implementação dos mecanismos de segurança, pois esses aspectos podem variar ao longo do tempo e da adoção de novas tecnologias. Existem algumas normas que definem os aspectos a serem levados em consideração para elaboração de políticas de segurança. Entre essas normas destacam-se a BS-7799 [21] e a NBR ISO/IEC 17799 [22].

De acordo com Crosbie [23], uma política de segurança define o que deve ser permitido e o que deve ser proibido em um sistema. Existem fundamentalmente duas correntes que podem ser usadas para escrever uma política de segurança.

A primeira descreve exatamente quais são as operações permitidas em um sistema e por consequência tudo que não é expressamente permitido, é proibido. A esta filosofia chamamos Proibitiva.

A segunda corrente, chamada Permissiva, descreve as operações proibidas em um sistema. Contrariamente à primeira, tudo que não é proibido, é permitido.

Segundo Ned [24], uma política de segurança pode ser descrita em seis elementos básicos, apresentados abaixo:

- Disponibilidade: o sistema deve estar disponível para uso quando requisitado. Dados críticos devem estar disponíveis ininterruptamente.
- Utilização: o sistema deve ser utilizado somente para os objetivos que lhe foi designado.
- Integridade: o sistema e os dados devem estar íntegros e acessíveis a qualquer momento.
- Autenticidade: o sistema deve ser capaz de verificar a identidade do usuário, e este por sua vez, ter condições de analisar a identidade do sistema.
- Confidencialidade: dados privados devem ser acessados somente pelos seus donos ou por grupos autorizados por ele.
- Posse: o dono do sistema deve ter condições de controle do sistema.

Com o intuito de tornar uma política de segurança viável a longo prazo, é necessário uma certa flexibilidade no que diz respeito ao conceito de segurança arquitetural, tornando a política independente de hardware ou software específico. Todos os mecanismos para

a atualização da política devem estar claros e especificados, incluindo o processo e as pessoas envolvidas.

É necessário reconhecer que existem exceções para as regras e sempre que possível a política deve explicitar essas exceções. Por exemplo, um administrador do sistema pode ter o direito de pesquisar nos arquivos de um usuário. Podem haver casos onde múltiplos indivíduos terão acesso ao mesmo usuário, por exemplo, a senha de um usuário *root* ser compartilhada entre os administradores do sistema.

Outra consideração que deve ser feita é refente ao que pode acontecer a um sistema se um administrador repentinamente não esteja disponível para sua função (ficou doente ou deixou a organização). Se por um lado existe uma segurança maior na mínima disseminação de informações cruciais, pelo outro existe o risco de se perder essa informação crítica quando não compartilhada. Sendo assim, é necessário determinar o peso ideal desta medida para o sistema e especificar na política de segurança.

5.3 Métodos de Ataque

5.3.1 Ataques Gerais

De uma forma geral, um servidor DNS é suscetível a falhas e ataques como qualquer outro computador conectado à rede. Dessa maneira, um computador disponibilizando o serviço DNS aos usuário da Internet pode sofrer tentativas de ataques que utilizam-se de vários métodos.

Na maioria das vezes um servidor DNS é de propriedade de uma empresa ou instituição. Essa entidade administra os recursos e configurações referentes a este serviço. E como toda e qualquer instituição ela pode sofrer ataques de engenharia social visando a obtenção de informações para um acesso não autorizado aos servidores.

Esse tipo de ataque é muito frequente, não só na Internet, mas no dia-a-dia das pessoas. A grande maioria das empresas investes milhões em tecnologia de segurança da informação e proteção de seus sistemas mas esquecem de proteger seus colaboradores das armadilhas de engenharia social. [25]

Dessa maneira, engenharia social consiste nas artimanhas e métodos usados para enganar ou explorar a confiança das pessoas com a intenção de obter informações sigilosas e sensíveis, ou ainda, induzir as pessoas a executar ações que enfraqueçam a segurança. Para obter tais tipos de informações, o indivíduo pode se passar por outra pessoa, assumir

outra personalidade, fingir ser um profissional de determinada entre outros.

O primeiro passo para um ataque de engenharia social é a pesquisa, na maioria das vezes pela Internet, da intituição ou alvo do ataque. O próximo passo é a preparação do ataque podendo ser via telefone ou via email.

Na abordagem, para se descobrir uma senha ou nome de usuário, o método mais simples, mais usado e mais eficiente que é utilizado é a pergunta direta. Se o colaborador da instituição não estiver preparado, a possibilidade de o atacante obter a resposta positiva é certa e assim o atacante ganha acesso ao sistema. Mas também existem ataque mais complexos e demorados, envolvendo diversas etapas e planejamentos elaborados, bem como uma combinação do conhecimento da manipulação e tecnologia.

Um caso verídico envolvendo engenharia social, relatado no livro "A Arte de Enganar"[26] e no filme "Takedown"(2000), mostra os fatos ocorridos na vida de Kevin Mitnick, suas invasões aos sistemas da DEC (do inglês, *Digital Equipment Corporation*) e a sua maestria ao efetuar ataques de engenharia social.

Outra ofensiva muito utilizada para o acesso a computadores de uma rede é o ataque por força bruta. Geralmente tem como objetivo descobrir a senha de um usuário, entretanto seu uso pode se extender a outras áres, por exemplo, a colisão de *hash*.

De acordo com Ranghetti e Milnitsky [27], força bruta é um ataque trivial e de uso geral baseado na premissa de enumerar todas as possíveis soluções e verificar se cada uma satisfaz o problema. A solução sempre será encontrada se existir, entretanto o custo computacional para testar todas as possíveis soluções é muito alto e por isso este tipo de abordagem é utilizada em problemas onde é sabido que o seu grau de complexidade é reduzido.

Uma variante do ataque por força bruta é o ataque por dicionário. Ao contrário da primeira abordagem que utiliza todas as possibilidades de caracteres, o ataque por dicionário utiliza um arquivo que contém diversas palavras e expressões para fazer o teste. Assim como o ataque anterior, o ataque de dicionário irá testar cada palavra até obter sucesso ou esgotarem-se os termos.

Uma outra abordagem de ataque é o chamado monitoramento de toques do teclado. Esta abordagem é muito utilizada para a captura de dados de computadores pessoais, mas também é válida se aplicada sobre os computadores de uma rede corporativa para obtenção de senhas ou informações que possam induzir a uma possível solução.

Este ataque é muito comum em diversos sistemas operacionais, onde um programa é

instalado no computador sem o conhecimento do usuário e este passa a gravar todos os toques do teclado em um arquivo escondido. Após um determinado período de tempo o atacante obtém o arquivo salvo com todos os dados digitados pelo usuário. [28]

Existem muitos outros tipos de ataques que podem ser executados visando o acesso a um determinado computador da rede. As abordagens de ataque relatadas atuam mais sobre a falha no lado humano e não necessariamente sobre falhas e vulnerabilidades dos sistemas ou protocolos.

Nas próximas seções serão introduzidos os principais ataques relacionados ao serviço DNS que atuam diretamente sobre falhas e vulnerabilidades dos sistemas ou protocolos que cercam o DNS.

5.3.2 Negação de Serviço (DoS)

Ataques de negação de Serviço ou ataques DoS (do ingês, *Denial of Service*) como também são conhecidos, são táticas de ataque caracterizadas por uma tentativa de impedir que usuários legítimos utilizem um determinado serviço. Em alguns casos, o ataque de negação de serviço pode fazer parte de um ataque maior, sendo utilizado para desabilitar algum serviço ou sistema de segurança que esteja impedindo o acesso do invasor ao sistema. [29]

Este tipo de ataque não tem como objetivo invadir uma rede ou roubar informações privilegiadas, e sim bloquear o acesso dos usuários a um determinado serviço. É muito comum, neste tipo de ataque, o alvo ser um servidor web que depois de receber o ataque tornará o acesso as suas páginas webs indisponíveis.

Segundo Bauer [30], durante um ataque de negação de serviço toda a banda disponível para acesso ao computador ou rede é ocupada acarretando uma grande lentidão ou até mesmo indisponibilizando qualquer comunicação com os recursos da rede.

Existe ainda uma variante do ataque DoS que é chamada de DDoS (do inglês, *Distribuited Denial of Service*). Este ataque, ao contrário do DoS, tem como origem vários computadores de locais variados o que dificulta muito o rastreamaneto e combate.

Este tipo de ataque também pode vitimar servidores DNS que oferecem o serviço à Internet ou rede. Contudo, as extensões de oferecidas pelo DNSSEC não visam garantir a segurança e proteção quanto a este tipo de ofensiva. Este é um outro tema a ser abordado mas transcende aos limites de escopo propostos por este trabalho ficando apenas relatado

ao final do documento no capítulo "Trabalhos Futuros".

Nas seções a seguir, será dado o enfoque às principais abordagens de ataques que se utilizam de falhas nos sistemas ou nos protolocolos com finalidade de manipular os dados das respostas DNS afim de iludir o requisitante.

5.3.3 *Man In The Middle*

O ataque *Man in the middle,* ou na tradução livre "Homem no Meio", consiste basicamente em o atacante se colocar entre o usuário e o servidor, forjando ser este último. Durante o ataque, a comunicação entre o cliente e o servidor é interceptada e de posse da informação o atacante pode retransmitir os dados de forma transparente, com modificação ou bloquear a mensagem.

De acordo com Schmoyer, Lim e Owen [31], durante o ataque man-in-the-middle a comunicação é interceptada pelo atacante e retransmitida por este de uma forma discricionária. O atacante pode decidir retransmitir entre os legítimos participantes os dados inalterados, com alterações ou bloquear partes da informação. Como os participantes da sessão, o cliente e o servidor, não distinguem que os dados recebidos estão adulterados, acabam por tomar esses dados como verdadeiros fornecendo informações ou executando instruções por ordem do atacante.

A figura abaixo ilustra o cenário de um ataque de homem no meio básico, mostrando a interceptação da comunicação entre o usuário e o servidor.

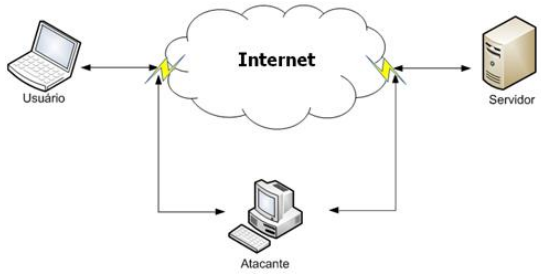

Figura 13: Ataque do Homem no Meio

Este tipo de ataque é considerado um ataque genérico, pois há várias vertentes a serem exploradas dentro do seu contexto e é a abordagem utilizada no ataque de envenenamento de cachê em servidores DNS

5.3.4 Envenenamento de IP

O envenenamento de IP na resolução de nomes de domínios ocorre quando é enviada uma resposta falsa a uma requisição de resolução de nome para o servidor DNS, fazendo com que ele armazene em cachê um endereço IP falso para um determinado nome de domínio. [32]

Quando um servidor DNS faz uma requisição a um outro servidor, questionando o IP de um determinado nome de domínio, ele aguarda até que receba uma resposta do mesmo. Ao receber uma resposta, ele verifica se determinadas informações estão corretas e, em caso positivo, armazena a resposta em seu cachê.[33]

Segundo Ferraz [34], devido as características do protocolo IP, o reencaminhamento de pacotes é feito com base numa premissa simples: o pacote deverá ir para o destinatário (endereço-destino) e não há verificação do remetente (não há validação do endereço IP nem relação deste com o *router* anterior). Dessa maneira, é trivial a falsificação do endereço de origem através de uma manipulação simples do cabeçalho IP.

Um ataque de envenenamento visa antecipar uma resposta de resolução de nome falsa para um servidor DNS vítima, assim a resposta DNS enviada pelo atacante precisa obrigatoriamente chegar antes que a resposta verdadeira enviada pelo servidor DNS questionado. Desta maneira, mesmo que a resposta DNS enviada pelo atacante chegue primeiro, logo em seguida o servidor alvo do ataque receberá a resposta de resolução de nome oriunda do servidor DNS verdadeiro. Como servidor alvo recebeu uma resposta com as informações esperadas ele irá desprezar as demais respostas.

De acordo com Vagner Sacramento e Cláudio Monteiro [35], as informações a serem verificadas na resposta obtida são:

- Se o campo ID e o campo "Nome a Ser Resolvido"do pacote DNS são iguais aos enviados na requisição;
- Se a porta de origem é igual à porta de destino do pacote UDP enviado na requisição;
- Se o endereço IP de origem é igual ao endereço IP de destino enviado na requisição.

Supondo que uma resposta válida tenha sido enviada por um indivíduo malicioso, que se passa pelo servidor DNS questionado, as informações contidas na resposta recebida podem estar incorretas e farão com que o servidor DNS as armazene em seu cachê. Desta maneira, o envenenamento de IP em servidores DNS acaba poluindo o cachê do DNS

vítima com informações errôneas e enquanto permanecerem ativas no cachê serão repassadas, aos requisitantes, como sendo verdadeiras. A figura abaixo demonstra um cenário de um ataque de envenenamento de IP.

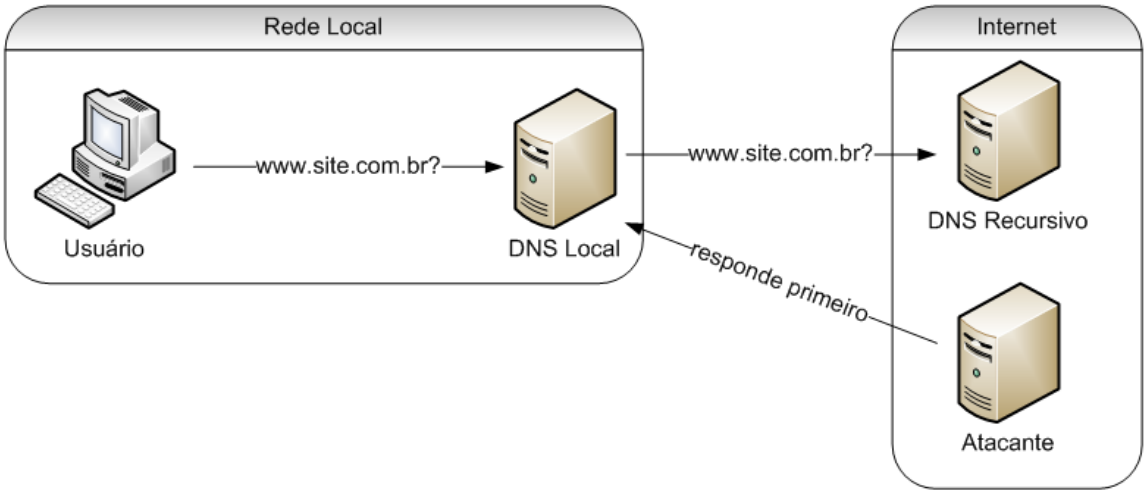

Figura 14: Envenenamento de IP

Várias consequências podem ser exploradas a partir da aplicação deste ataque. Algumas delas são [33]:

- Alteração da origem da informação requisitada na abertura de uma página web.

  Com um ambiente previamente preparado pelo atacante quando o usuário entrar com um endereço de uma página web que deseja visitar (o site de uma instituição bancária, por exemplo) ele pode ser redirecionado para uma página devidamente preparada. Esta página fica hospedada em um servidor web informado pelo atacante através do endereço IP utilizado como resposta na resolução de nome que foi efetuada. Ou seja, o site que será exibido ao usuário pode ser um site clonado e preparado para obter seus números de contas bancárias e senhas do usuário. Neste cenário, as consequências poder ser desastrosas.

- O envenenamento de IP pode ser utilizado para driblar mecanismos de defesa baseados em *wrappers* (mecanismos de softwares usados para filtrar a utilização de serviços como telnet, ftp, talk, etc) que utilizam o nome do *hosts* para verificar a autenticidade entre eles.

- Ataque a todas as aplicações (e-mail, web, ftp, etc) que usufruem do serviço DNS para tradução de nomes.

A execução bem sucedida de um ataque de envenenamento de DNS pode gerar inúmeras consequências não deixando nenhum rastro ou possibilidade de identificação do indivíduo atacante. É impraticável a detecção da identidade do atacante, pois este, em geral, falsifica o endereço de origem dos pacotes na resposta de resolução de nomes enviada ao servidor DNS vítima.

A partir de estratégias e artifícios elaborados e relatados em [33] é possível implementar ataques deste gênero, localmente ou remotamente, nas aplicações que implementem o protocolo DNS e comprovar a eficiência e consequências do ataque descrito.

5.4 Mecanismos de Segurança

Segundo Gomes e Farias [36], ao conectar um computador à uma rede, é necessário tomar certas providências para garantir e certificar que esta nova máquina conectada possam não vir a ser uma portão de entrada para invadores procurando prejudicar os sistemas ou a rede.

Frente a isso, faz-se necessário a aquisição de ferramentas, políticas e mecanismos de segurança que possam garantir uma rede segura a todas as estações de trabalho e servidores que nela se conectem.

Neste sentido, algumas diretivas de segurança podem ser implementadas visando a integridade, autenticidade e confiabilidade dos dados e acessos que ocorrem na rede. Entre os mecanismos mais utilizados e difundidos destacam-se a assinatura digital, o processo de autenticação e autorização, controle de acesso, *firewalls*, entre outros.

Segundo Balparda [5], as assinaturas digitais são feitas para que uma entidade possa, digitalmente, "assinar"um documento. Espera-se que uma assinatura eletrônica tenha as mesmas características de uma assinatura do mundo real:

- Seja fácil de produzir para quem assina;
- Seja fácil de verificar por qualquer um;
- Seja muito difícil de ser falsificada;
- Tenha uma vida útil apropriada (de modo que quem assine não possa negar ter assinado);

Uma assinatura digital não é feita para proteger uma mensagem contra um indivíduo malicioso. Ela é feita para garantir que um determinado indivíduo realmente efetuou o processo de assinatura sobre a mensagem ou texto. Todos que quiserem verificar a assinatura terão que ter acesso à assinatura e à mensagem. Neste caso, o indivíduo poderá ter acesso à assinatura e poderá executar a verificação da mesma. A idéia é evitar apenas que se falsifique uma assinatura.

Quando se assina um documento físico, o que se assina efetivamente é o próprio papel. O papel, neste caso, é a entidade que faz a ligação entre a assinatura propriamente dita e a informação contida no papel. A assinatura manuscrita é considerada uma forma de medida biométrica indireta, uma vez que imprime no papel uma escrita que tem uma certa dependência das biocaracterísticas de uma pessoa. Dessa maneira, existe uma ligação entre o signatário e o documento no papel. O mesmo não ocorre em documentos digitais.[37]

Uma assinatura digital é código binário criado a partir do documento e de alguma informação que associe a assinatura a um determinado indivíduo. Essa associação é chamada de autenticação e é feita em três níveis básicos:

- Algo que se sabe, uma senha ou palavra por exemplo;
- Algo que se possui, um cartão magnético ou *token*;
- Algo que se é, uma medida biométrica do indivíduo.

Somente um tipo de autenticação pode não ser considerado seguro o suficiente. Por este motivo, às vezes, é utilizado mais de uma dessas formas para aumentar o grau de associação. É muito comum as instituições bancárias utilizarem algo que se sabe (uma senha) com algo que se tem (um cartão) para liberar o acesso a sua conta.

A utilização da assinatura digital providencia a prova irrefutável de que a mensagem foi enviada pelo emissor que assinou o documento. Para que este requisito possa ser verificado e comprovado, uma assinatura digital deve ter as seguintes propriedades básicas:

- Autenticidade: garantia da identidade de quem executou a transação;
- Integridade: garantia de que o conteúdo da transação não foi alterado;
- Não-repúdio: garantia que impede uma entidade participante numa dada operação de não negar essa participação

Para que estes princípios sejam garantidos é indispensável a utilização de soluções que garantam confiança nas transações eletrônicas. A infraestrutura de chaves públicas aliada a criptografia assimétrica e aos resumos criptográficos é considerada uma das melhores opções.[7]

Para realizar a verificação da assinatura digital é necessário obter o documento assinado. Este documento é composto por duas partes básicas: a mensagem e o *hash* da mensagem cifrado com a chave privada do signatário. Utilizando a chave pública do signatário é possível decifrar o resumo assinado e obter o original. Ao mesmo tempo, de posse do documento original, basta submetê-lo ao algorítmo de resumo criptográfico para obter o *hash*. O resultado da comparação entre o resumo do documento original e o resumo decifrado precisa ser igual para que a assinatura seja íntegra. A imagem abaixo ilustra o processo de verificação de uma assinatura digital.

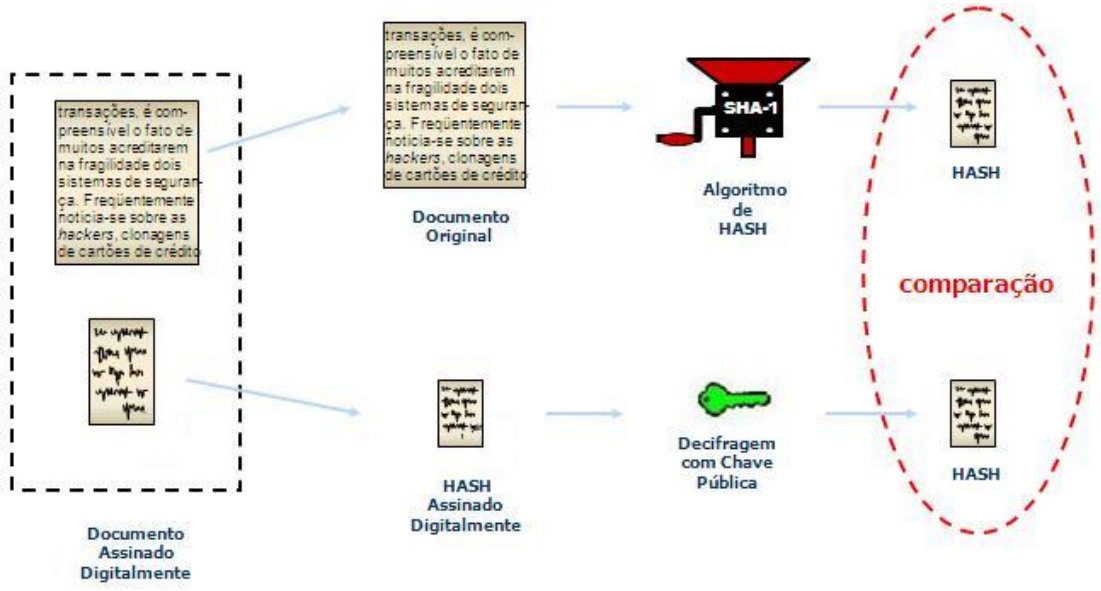

Figura 15: Verificação de uma assinatura digital - retirado de [7]

Autenticação é a ação de confirmar algo ou alguém, que reivindica a autoria ou veracidade, como autêntico. Também pode remeter a confirmação da procedência de um indivíduo frequêntemente relacionado com a verificação da sua identidade.

A autenticação é a técnica através da qual um processo confirma que seu parceiro na comunicação é quem deve ser e não um impostor. A autenticação lida com a questão de determinar se você está ou não se comunicando com um processo específico. Confirmar a identidade de um processo remoto, face à presença de um intruso ativo mal-intencionado, é surpreendentemente difícil e exige protocolos complexos baseados no uso da criptografia.[1]

Autorização é o mecanismo pelo qual é possível garantir que apenas indivíduos autorizados utilizem os recursos protegidos de uma rede ou sistema computacional. O processo de autorização é que verifica se o indivíduo requisitante possui permissões de acesso compatíveis com o recurso que está tentando acessar.

Segundo Tanenbaum [1], a autorização se preocupa com o que o processo ou indivíduo tem permissão para fazer no sistema. Por exemplo, um processo cliente entra em contato com um servidor de arquivos e afirma: "Sou o processo X e quero excluir o arquivo Y". Do ponto de vista do servidor de arquivos, as seguintes questões devem ser respondidas:

1. Esse processo é realmente o processo X (autenticação)?
2. X tem permissão para excluir o arquivo Y (autorização)?

Somente quando ambas as respostas das perguntas acima forem afirmativas e sem qualquer ambiguidade, a ação solicitada poderá ser executada.

No conxteto de segurança da informação, o controle de acesso é a capacidade de limitar ou controlar o acesso aos recursos. Para tal, cada indivíduo requisitante, deve ser primeiramente identificado ou autenticado de forma que os direitos e permissões de acesso sejam atribuídos ao usuário. Basicamente o controle de acesso é responsável por definir quais recursos estão disponíveis para acesso, quais são as operações que podem ser executadas nestes recursos, quais são os componentes autorizados a desempenhar tais operações. Pode ser classificado quanto:

1. à centralização do controle: Centralizado ou Descentralizado;

   Controle de Acesso Centralizado: nesse tipo de controle, uma entidade central (sistema ou usuário) toma as decisões sobre acesso aos recursos. Como vantagem, ele garante a padronização do acesso às informações, e impede a superposição de direitos. Como desvantagem, a falha no sistema central impede qualquer acesso às informações.

   Controle de Acesso Descentralizado: nesse tipo, o controle é delegado a entidades mais próximas dos recursos que podem gerenciar melhor os problemas com os recursos sob sua supervisão. Como vantagem, a falha em um sistema de controle de acesso a um recurso não interfere no acesso aos demais recursos. Como desvantagem a perda da padronização do acesso às informações, e a possibilidade de superposição de direitos, que causam furos de segurança.

2. ao controle pelo sistema: Mandatório ou Discricionário;

   Controle de Acesso Mandatório: a política de acesso é determinada pelo sistema e não pelo proprietário do recurso. Nesse tipo de controle há a construção de um sistema que manipula múltiplos níveis de classificação entre sujeitos (nível de privilégios) e objetos (nível de sensibilidade da informação). Os administradores dos sistemas definem os níveis de privilégio dos usuários e a política de acesso. Já os gestores das informações estabelecem a rotulação das informações quanto ao seu nível de sensibilidade. Por último, cabe ao sistema cuidar de aplicar as regras da política com base nos privilégios dos usuários e no rótulo das informações.

   Controle de Acesso Discricionário: a política de controle de acesso é determinada pelo proprietário do recurso. O proprietário do recurso decide quem tem permissão de acesso a determinado recurso e qual privilégio ele tem. Esse tipo de controle tem como premissas: todo objeto em um sistema deve possuir um proprietário, logo um objeto sem proprietário não é protegido e direitos de acesso e permissões podem ser dados pelo proprietário do recurso a usuários individuais ou grupos de usuários.

3. ao mecanismo de controle: baseado em regras ou em perfis.

   Controle de Acesso Baseado em Regras: o acesso é definido pela lista de regras estipuladas pelo administrador do sistema, de acordo com a rotulação da informação e o nível de privilégio do usuário.

   Controle de Acesso Baseado em Perfis: o acesso às informações é baseado no cargo do usuário ou ao grupo que o usuário pertence. São definidos papéis genéricos com os respectivos privilégios e a determinação do perfil de um usuário é feita de forma discricionária pelo gestor de um recurso.

Existe a possibilidade de controlar o roteamento de uma rede, especificando as rotas preferenciais ou obrigatórias para a transferência de dados ou acessos ao sistema. Este artifício pode ser utilizado para garantir que as informações trafeguem por rotas fisicamente seguras ou para garantir que informações sensíveis utilizem-se de canais de comunicação que forneçam os níveis apropriados de segurança.

Na ocorrência de tentativas de acessos indevidos ou erros no sistema, é de grande importância que o registro dessas informações sejam armazenados para futuras verificações.

A detecção de eventos em um sistema deve incluir desde eventos normais e esperados pelo sistema, como um acesso bem sucedido de um usuário, quanto uma detecção de aparentes tentativas de violações de segurança. É recomendado que o mecanismo de

detecção tenha o apoio de um componente de gerenciamento para determinar quais os eventos que devem ser detectados.

O registros desses eventos possibilitam a detecção e investigação de possíveis violações de segurança em um sistema e também a realização de auditorias de segurança. Ao executar uma auditoria faz-se uma revisão e exame dos registros das atividades do sistema com o objetivo de comprovar a eficácia dos mecanismos de controle do sistema para: garantir a compatibilidade entre a política de segurança e os procedimentos operacionais, auxiliar na avaliação de danos e riscos, recomendar modificações nos mecanismos de controle, na política de segurança e nos procedimentos operacionais do sistema.

A auditoria de segurança envolve duas tarefas:

1. O registro dos eventos no arquivo de auditoria de segurança (security log);
2. Análise das informações armazenadas nesse arquivo para a geração de relatórios.

Cabe deixar claro que a segunda tarefa, de análise, é uma função de gerenciamento de segurança e não um mecanismo automático. Os mecanismos de arquivamento de informações para auditoria de segurança, usados na primeira tarefa, devem permitir informar quais dados serão registrados, sob que condições serão registrados, além de uma definição de sintaxe e semântica para representá-los.

A maioria dos mecanismos citados se referem à segurança relativa aos acessos que ocorrem na rede e aos dados que nela trafegam. No contexto de requisições DNS que extrapolam redes privadas e públicas, é indispensável que os dados das respostas estejam íntegros, autênticos e confiáveis. Fundamentado nos capítulos anteriores percebe-se que as extensões de segurança oferecidas pelo DNSSEC se mostram eficazes na resolução do problema.

5.5 Considerações de Segurança

5.5.1 Segurança em Servidores Autoritativos

Um servidor autoritativo autorizado pelo Registro.br para responder por um domínio, deve ficar disponível para qualquer consulta feita na Internet. Ou seja, ele é um servidor aberto, sob o ponto de vista de consultas aos domínios.

Do ponto de vista da segurança computacional isto é muito perigoso. Segundo os comprovados argumentos de Dan Kaminsky, cujos artigos e experimentos podem ser vistos em [38], se o servidor autoritativo não estiver muito bem preparado e, não usar o DNSSEC, sua vulnerabilidade passa a ser enorme e ele está suscetível à chamada poluição de DNS. Felizmente a era pós-Kaminsky trouxe melhoras significativas nos sistemas que implementam o autoritativo, principal alvo de ataques.

5.5.2 O Registro DS - DNSSEC

O registro DS aponta para uma DNSKEY usando um resumo criptográfico, o tipo do algorítmo da chave e o identificador da chave. O registro DS destina-se a identificação de uma chave existente, mas é teoricamente possível para um atacante gerar uma chave que coincida com os campos do DS. Essa possibilidade depende do tipo do algorítimo de *hash* utilizado.

Atualmente, o único algorítmo de *hash* definido para uso no registro DS é o SHA-1, e o grupo de trabalho (responsável pela definição, padronização e escrita das RFC referente ao DNSSEC) acredita que construir uma chave pública que corresponda ao algoritmo, identificador e *hash* encontrados em um registro DS é difícil o bastante que um tal ataque não é uma séria ameaça neste momento. [39]

5.6 Conclusão

Todo e qualquer computador plugado à uma rede de computadores está, de certa forma, exposto a ataques. Estes ataques podem ocorrer devido a falhas humanas ou vulnerabilidades nos sistemas e protocolocos.

Muitas das tecnologias apresentadas solucionam parte dos problemas de segurança encontrados. Neste contexto, o DNSSEC se mostra a melhor solução para o impace computacional referente a resolução segura de nomes. No próximo capítulo será abordado o modo de funcionamento do DNSSEC, suas requições e respostas, em comparação com o seu predecessor, o DNS.

6 Funcionamento do DNS e do DNSSEC

6.1 Introdução

Esta seção irá demonstrar, com a ilustração de figuras e esquemas, o funcionamento básico do DNS e do DNSSEC e como eles fazem a resolução dos nomes através de servidores autoritativos e recursivos. Para fins acadêmicos será utilizado um cenário básico com um servidor recursivo que responde ao cliente e três servidores autoritativos responsáveis por ".", "br"e "edu", respectivamente. Também será desprezada a utilização de cachê nos servidores DNS. Nos exemplos a seguir os clientes pedem a resolução de nome para o domínio "exemplo.edu.br".

6.2 DNS

O cliente solicita ao servidor DNS a resolução do domínio "exemplo.edu.br"e este por sua vez repassa a requisição ao servidor raiz (responsável pelo "."). O servidor raiz não é responsável por resolver este domínio e então repassa ao servidor recursivo a referência do próximo servidor da hierarquia.

No próximo passo o servidor recursivo utiliza a referência obtida do servidor raiz, no caso o servidor responsável pelo "br", e solicita a ele a resolução do domínio. O servidor neste nível hierárquico também não é responsável pela resolução do domínio e devolve uma referência ao servidor do próximo nível.

No último passo, o servidor recursivo solicita ao servidor de terceiro nível a resolução do domínio. Este servidor é o responsável e sabe como resolver o endereço. Ele retorna ao servidor requisitante o IP relacionado ao domínio. Agora de posse do IP do domínio o servidor recursivo pode informar ao cliente o IP para que este se conecte ao site. A figura 16 demonstra as etapas de funcionamento do DNS descrita nos passos anteriores.

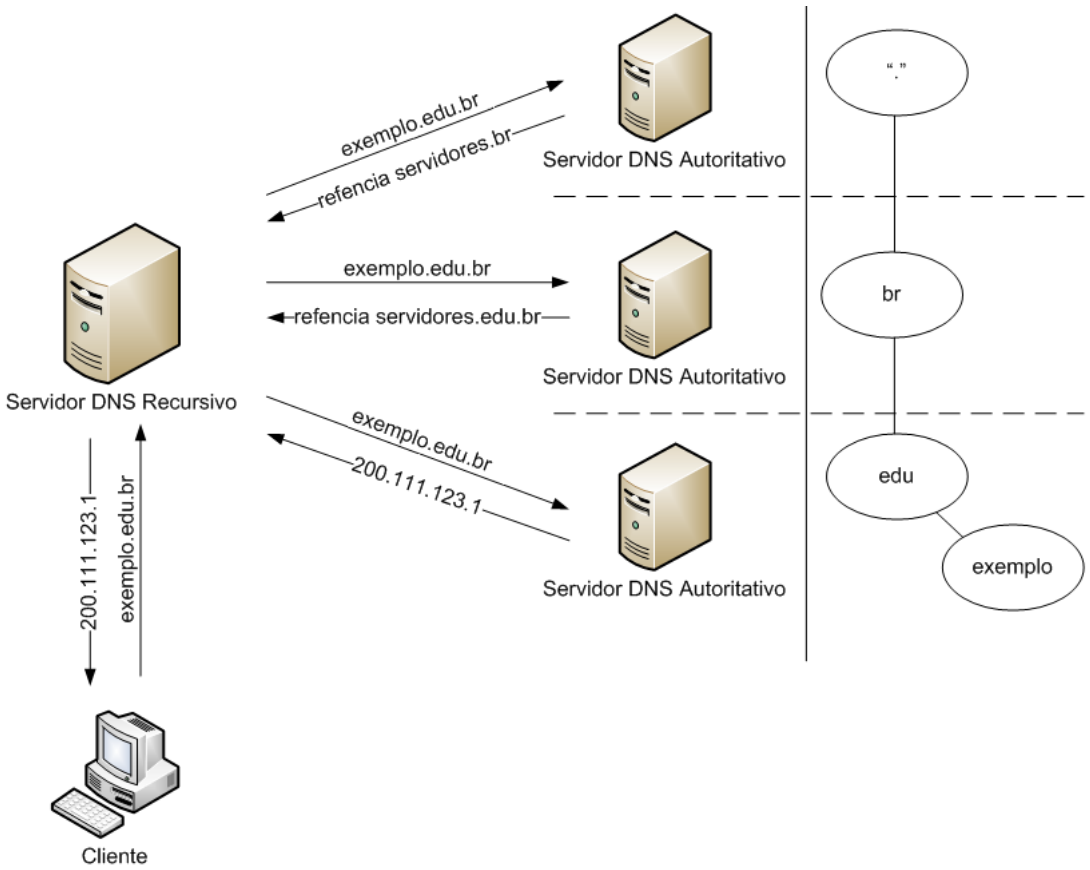

Figura 16: Funcionamento básico de uma requisição do DNS

6.3 DNSSEC

O cliente solicita ao servidor recursivo a resolução do nome "exemplo.edu.br". O servidor recursivo já possui a chave pública do *root server* e recebe deste a referência para o próximo servidor na hierarquia. Essa refêrencia está assinada e o recursivo utiliza a chave pública para verificar a assinatura digital presente. Se a verificação obtiver sucesso, o processo continua e caso o contrário é encerrado. O mesmo ocorre para todas as outras verificações de chaves e assinaturas.

Na próxima etapa, o servidor recursivo requisita a chave pública do servidor que constava na referência do *root server* e utiliza-se do registro DS, também obtido na referência do *root server*, faz a comparação das chaves. Após a comparação das chaves, a requisição de resolução de nomes é efetivamente remetida ao servidor da zona "br", este por sua vez, não é responsável pela resolução e retorna um registro NSEC (*Next Secure)* com autoridade sobre um registro DS (ambos assinados). Novamente ocorre a verificação da assinatura.

Na última etapa, o servidor recursivo agora possui a referência para o servidor da

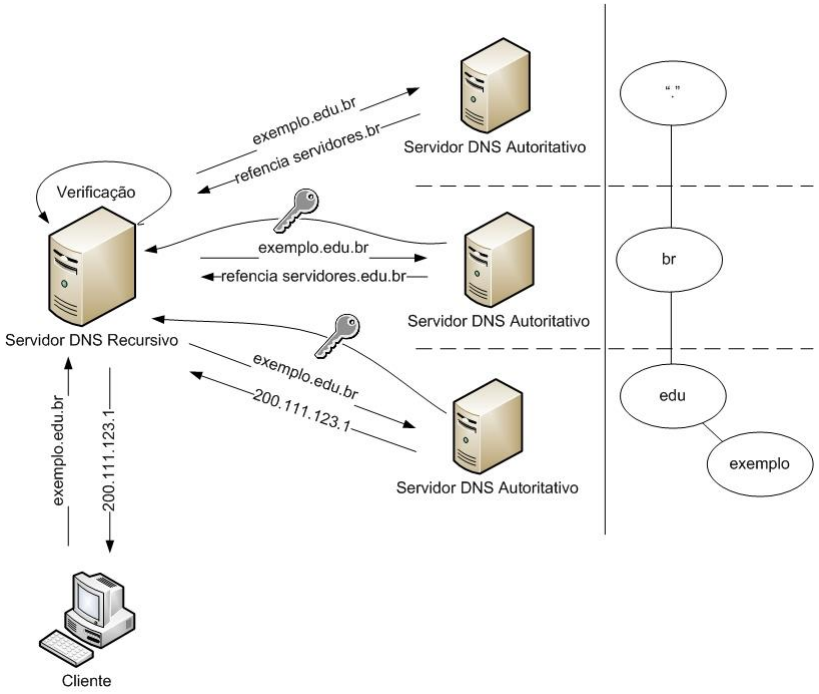

Figura 17: Funcionamento básico de uma requisição do DNSSEC

zona "edu". Primeiramente ele faz a requisição da chave pública e logo em seguida a comparação da chave com o registro DS obtido anteriormente. Obtendo sucesso na comparação da chave, o servidor recursivo pede a resolução do dominínio e recebe uma resposta assinada da resolução apontando para o IP do domínio. É feito uma última verificação da assinatura e em seguida é devolvido ao cliente a resposta contendo o IP do domínio "exemplo.edu.br". A figura 17 demonstra as etapas de funcionamento do DNSSEC recém descritas.

6.4 Comparação

A figura abaixo coloca lado a lado o processo de resolução de nomes executado pelo DNS e pelo DNSSEC. É possível observar as trocas de chaves e de registros na execução do protocolo DNSSEC. Outra questão que fica evidenciada é referente ao tamanho e quantidade de requisições/respostas.

Enquanto o DNS utilza oito pacotes para envio das requisições e das respostas o DNSSEC utiliza-se de doze pacotes para o envio das chaves, requisições e respostas. O tamanho final dos pacotes do DNSSEC também são superior, cerca de seis vezes maior, devido ao seu conteúdo com assinaturas digitais. A figura abaixo expões a comparação de funcionamento entre o DNS e DNSSEC.

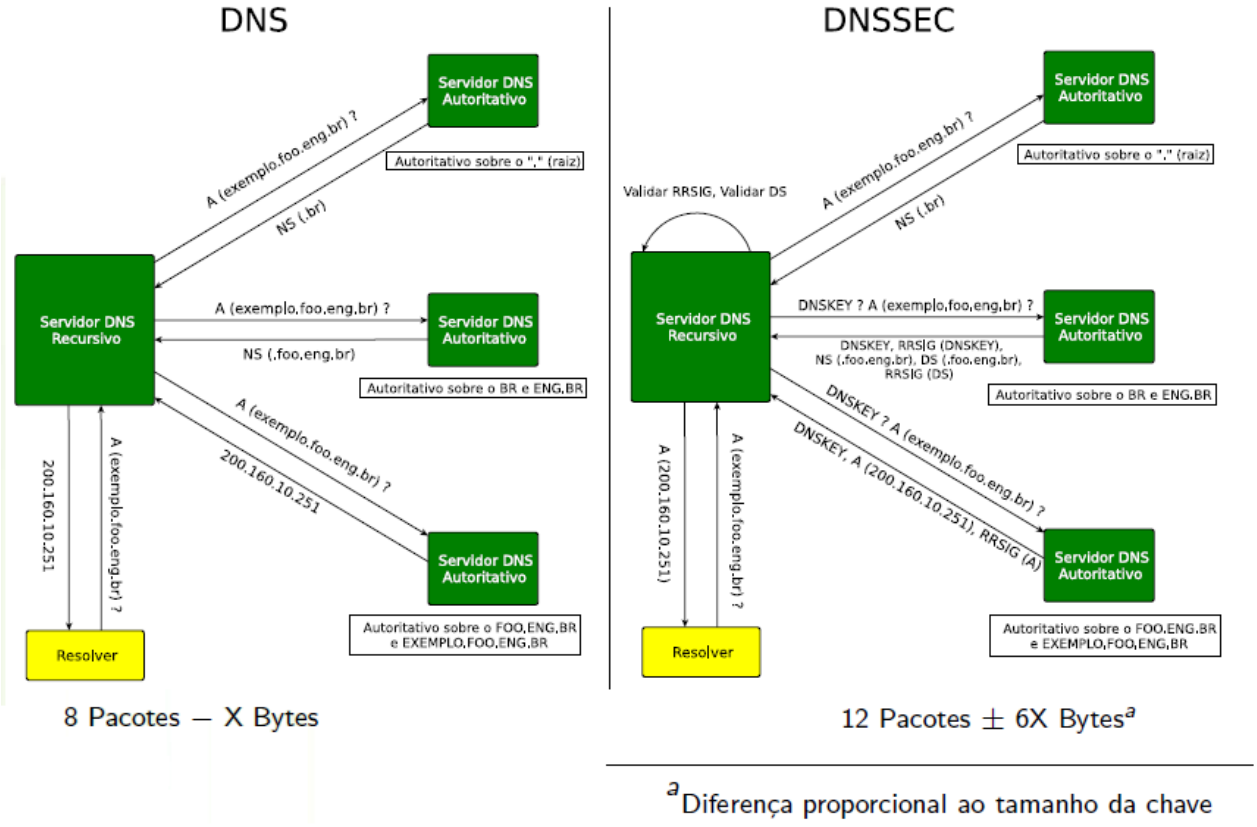

Figura 18: Comparação DNS e DNSSEC - retirado de [40]

6.5 DNSSEC ou SSL?

Ultimamente tem-se falado muito a respeito sobre qual a melhor maneira para se garantir o acesso seguro à um domínio. As questões levantas sempre giram em torno do uso do *Secure Socket Layer* (SSL) ou do DNSSEC. Mas qual das duas abordagens é a melhor e qual deve ser utilizada?

A resposta é muito simples - utilize os dois. A razão para isso é que cada uma das ferramentas resolve diferentes partes do problema.

O protocolo SSL é utilizado para a criptografia dos dados e a autenticação do domínio. Para garantir a autenticação o domínio precisa obter um certificado SSL emitido por uma Autoridade Certificadora. Esse certificado contém uma chave privada que é utilizada para estabelecer um canal seguro (chamado de sessão) entre o navegador do cliente e o website. Com essa sessão criada, todos os dados que trafeguem entre o cliente e o servidor estarão criptografados cifrados e seguros - no caso de haver um atacante bisbilhotando a rede e os pacotes que nela trafegam.

Contudo antes de se conectar a um website utilizando o SSL é necessário resolver o nome do domínio para saber em qual servidor está hospedado o sistema. Neste caso, é indicado a utilização o DNSSEC para uma resolução segura de nomes. Não só realizando a pesquisa de DNS mas também validando a assinatura da requisição que retornou do servidor, as extensões de segurança do DNS provêm um resolução segura e confiável. A validação e verificação das assinaturas ocorre em todos os níveis hierárquicos do DNS, desde os *root servers* até os *top level domain* (por exemplo, .org ou .edu) e se todas as assinaturas são válidas, então a resposta é enviada de volta ao cliente que agora pode se conectar ao site (e talvez usar o SSL).[41]

Se no primeiro passo o DNSSEC garante uma resolução de nomes confiável, indicando precisamente qual é o servidor que você quer acessar, o próximo passo é a utilização do SSL que garante a confiabilidade dos dados sensíveis que irão trafegar entre o seu computador e o sistema remoto. Dessa maneira a utilização das duas técnicas irá aumentar significativamente a segurança e causando o mínimo de exposição.

6.6 Conclusão

Como observado nas seções anteriores, o funcionamento do DNS e do DNSSEC são complementares. Enquanto o DNS é responsável pela resolução de nomes de domínios, as extensões DNSSEC promovem a validação e verificação de dados de forma confiável.

Também fica evidente que a utilização do DNSSEC não é a solução de todos os problemas de segurança. Sempre que utilizado em conjunto com outros mecanismos o grau de confiança dos dados obtidos será maior, como por exemplo a operação conjunta com o SSL garantindo uma resolução confiável e um canal seguro de conexão entre o cliente e o servidor.

7 *Prática e Demonstração dos Dados*

7.1 Introdução

Esta seção tem como objetivo relatar as principais etapas ocorridas na configuração dos servidores DNS para utilização do DNSSEC. Como forma de aprimoramento do entendimento, serão demonstrados exemplos de configurações de arquivos e comandos serão apresentados.

7.2 Configuração do Ambiente

Para a configuração e utilização do DNSSEC é necessário uma certa infraestrutura e alguns recursos. Para tal, foi utilizado um ambiente de rede com diversas máquinas, dois servidores DNS (*master* e *slave)* executando o BIND na versão 9.7 e também um domínio *brytec.com.br*. Esse cenário já é utilizado em produção tendo todas as suas zonas configuradas e funcionais. A proposta desta seção é configurar os servidores para utilizarem a resolução de nomes DNSSEC.

De acordo com o site do registro.br, o ".br"foi um dos pioneiros na adoção do DNSSEC em junho do 2007. Desde então, os interessados em utilizar o DNSSEC configuravam a chave KSK do ".br"em seus servidores DNS recursivos. Com a assinatura da raiz do sistema DNS, realizada na metade do ano de 2010, recomenda-se apena o uso da chave da raiz como *Trust Anchor* nas configurações dos servidores. A chave da raiz no formato de configuração do BIND (versão 9.7 ou superior) pode ser encontrada no site do registro.br e deve ser adicionada ao arquivo *named.conf* do servidor recursivo.

Na seção *options*, do arquivo *named.conf* é necessário habilitar a opção *dnssec-validation yes;* para que ocorra a validação das requisições DNS pelo servidor. A figura 19 exemplifica a habilitação da validação DNSSEC e e o ancoramento da chave do servidor

```
10 options {
11    // Relative to the chroot directory, if any
12    directory   "/etc/namedb";
13    pid-file "/var/run/named/pid";
14    dump-file   "/var/dump/named_dump.db";
15    statistics-file   "/var/stats/named.stats";
16    listen-on   { 127.0.0.1; 182.77.237.2; };
17    dns-validation yes;
18 };
19
20 // DNSSEC - Chaves publicas de consulta
21 trusted-keys {
22    . initial-key 257 3 8
23      "AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjF
24       FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoX
25       bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaD
26       X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz
27       W5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relS
28       Qageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulq
29       QxA+Uk1ihz0=";};
```

Figura 19: Adicionando a chave e habilitando a validação DNSSEC.

raiz.

A próxima etapa consiste na geração das chaves e para tal é utilizado o comando *dnssec-keygen*. De acordo com Camargo e Dantas [40], o Registro.br utiliza-se de quatro pares de chaves para assinatura em DNSSEC:

- KSK BR: *Key Signing Key* da zona BR. Sua chave privada é utilizada apenas para assinar o conjunto de chaves públicas da zona BR, ou seja, chaves públicas do KSK BR e ZSK BR. Este par de chaves fica armazenado em um HSM (do inglês, *Hardware Security Module*) conectado apenas ao servidor de publicação DNS. O algorítmo utilizado é o SHA-1 e o tamanho da chave é de 1280 bits.

- ZSK BR: *Zone Signing Key* da zona BR. Sua chave privada é utilizada para assinar registros da zona BR, conjunto de registros DS e NSEC. Essa chave é gerada em um servidor conectado apenas ao servidor de publicação, utiliza o algorítmo SHA-1 e o tamanho da chave é de 1152 bits.

- ZSK *.BR: *Zone Signing Key* de algumas das zonas abaixo de BR. Sua chave privada é utilizada para assinar registros das zonas assinadas: conjunto de registros destas zonas e conjunto de registros DS e NSEC. É gerada num servidor conectado apenas ao servidor de publicação, utiliza o algorítmo SHA-1 e o tamanho da chave é de 1024 bits.

- ZSK *,BR NSEC3 *Zone Signin Key* das zonas abaixo de BR. A chave é utilizada para assinar os registros autoritativos de todas as zonas br de segundo nível que

usam a tecnologia de assinatura SHA-1-NSEC3: registro dessas zonas e o conjunto de records DS e NSEC3. O par de chaves e gerado em um servidor conectado apenas ao servidor de publicação, utiliza o algorítmo SHA-1 e o tamanho da chave é 1024 bits.

Os servidores de geração de chaves e de armazenamento possuem um conexão com o servidor de publicação via cabo exclusivo que é utilizada somente para envio dos registros a serem assinados e para o recebimento das respectivas assinaturas.

Para a geração do par de chaves foi utilizado o comando *dnssec-keygen* com os seguintes parâmetros:

- -f : Define o tipo da chave
- -a : Algorítmo
- -b : Tamanho da chave (bits)
- -n : Especifica o tipo de dono da chave
- -r : Device de randomização

Em ambientes onde a geração de chaves se mostrar muito demorada pode ser necessário especificar um dispositivo de randomização. Estes dispositivos possuem funções capazes de gerar números pseudoaleatórios rapidamente. A figura abaixo exemplifica a geração das chaves.

```
dnssec-keygen -r /dev/urandom -f KSK -a RSASHA1 -b 1024 -n ZONE brytec.com.br

Generating key pair.....++++++ .....++++++
Kbrytec.com.br.+005+42199

cat Kbrytec.com.br.+005+42199.key

brytec.com.br. IN DNSKEY 257 3 5      AwEAAePpkLBaYj+NzSo388VFAEd+YjfRUixm4Zn4vJkPnPrkqWPeeCRs
                                      +eX5UGucxUtEDag7PDkC9hadMvAdHQbMtt8JS2sriE75BcLNCaJ+lkOe
                                      lqk16oCQEcpzpQ5Nh+vmoqJfiMYTlwwB3MdSwdTpsdWhEtziHOCK1tU8 xCa9foA7

cat Kbrytec.com.br.+005+42199.private

Private-key-format: v1.3 Algorithm: 5 (RSASHA1)
Modulus:            +mQsFpiP43NKjfzxUUAR35iN9FSLGbhmfi8mQ+c+uSpY954JGz55flQa5zFSOQNqDs8OQL2Fp0y8B0dBsy2
                    3wlLayuITvkFws0Jon6WQ56WqTXqgJARynOlDk2H6+aiol+IxhOXDAHcx1LB1Omx1aES3OIfQIrW1TzEJr1+gDs=

PublicExponent:     AQAB
PrivateExponent:    q+mP5BYpKbsyWHgf/lsP3N2uBGB11Vw9K8D9sY6fYHh+dQBoKOGwNhIa4TE9eIp6qr0TrgVXzrMAqz
                    GqpWhhPuqAGy6qGVqRNdg4kJKuLeyzbhOQkUt2us+UyVEgkwCBk3Svgjcc4SloyR8GGGL8VJcnLXJSMvtjoWDy1pOSZwE=
Prime1:             /rKF3F+3AM7+qFYkMhcO0LidFjybrL2HPMD9gqO+vy42MvugF89VoTxSd87FfR2EN64oCid5zAHORTjHW5jO+w==
Prime2:             5RP49pj1ky0UfMmSJa81flkJHXBTgNI/JHUCtQcZr/CF86y7ua9UfVkCa0gd8yMQUa/VswvPlRGNDIGg/lFPwQ==
```

Figura 20: Geração das chaves do DNSSEC.

Antes de assinar a zona é necessário incrementar o número serial do registro SOA para que ocorra a sincronização com os servidores secundários. Também é necessário incluir no arquivo de zona as chaves que serão utilizadas. A figura abaixo demonstra tais configurações.

Para realizar a assinatura da zona é utilizado o comando *dnssec-signzone*. Ao se assinar a zona são gerados os registros RRSIG e NSEC que serão ordenados de forma canônica dentro do arquivo da zona. A figura 21 demonstra a assinatura de uma zona.

Para efetuar a assinatura de uma zona foi utilizado o comando *dnssec-signzone* com os seguintes parâmetros:

- -S : busca as chaves da zona e determina como estas serão utilizadas;
- -z : Ignora o bit SEP da chave e assina toda a zona;
- o último parâmetro se refere ao arquivo de zona.

Após a assinar uma zona é gerado um arquivo contendo o registro DS que será usado para delegações. Também é necessário editar o arquivo *named.conf* alterando a referência para o arquivo de zona assinado e restartar o BIND.

É preciso atualizar o DS no sistema de provisionamento do registro.br informando o algorítmo e o *hash* contido no DS e esperar uma nova publicação (publicações a cada 30 minutos). A figura abaixo demonstra a tela do sistema do registro.br onde se cadastra o DS da zona.

Caso existam zonas delegadas que utilizem DNSSEC dentro do domínio, os registros DS destas zonas devem ser adicionados no arquivo de zona e este deve ser re-assinado.

7.3 Verificando a Resolução DNSSEC

Esta seção tem como objetivo demonstrar a utilização do programa DIG para realizar uma consulta DNS ao domínio *brytec.com.br* e *ufsc.br* apresentando os dados mostrando que os objetivos da instalação do DNSSEC foram alcançados.

O DIG é um programa para auxílio na gerência de redes de computadores, utilizado por administradores para realizar consultas sobre registros de DNS em um determinado domínio, *host* ou IP. Ele realiza pesquisas DNS e exibe as respostas retornadas do servidor de nome que foi consultado.

```
$ dnssec-signzone -S -z brytec.com.br

Verifying the zone using the following algorithms: RSASHA1.
Zone signing complete:
Algorithm: RSASHA1: KSKs: 1 active, 0 stand-by, 0 revoked
                    ZSKs: 0 active, 0 stand-by, 0 revoked
brytec.com.br.zone.signed

$ cat brytec.com.br.zone.signed
brytec.com.br.      3600    IN SOA    brytec.com.br. admin.brytec.com.br. (
                    2010083102 ; serial
                    10800      ; refresh (3 hours)
                    1800       ; retry (30 minutes)
                    2419200    ; expire (4 weeks)
                    81400      ; minimum (22 hours 36 minutes 40 seconds)
                    )
3600    RRSIG    SOA 5 3 3600 20101202201350 (          20101102201350 42199 brytec.com.br.
                                                        1EEfC7Ndp9hiS/FNen/BLq3z3vBvL+qE3u57
                                                        6xO4WH3kD0VTdIo8nActmaxpQVkJkjrzkOma
                                                        PfbpwsoOtd87ttiFij/rlQw6nRkKpFDcOjMX
                                                        ojF0OxxcZ+ut66wYB7TbEWdcGj/xTf5bK0MZ
                                                        Pk4f5M+eBDfD7HSKAf+gezjIiJM= )

81400    NSEC    brytec.com.br. SOA RRSIG NSEC DNSKEY
81400    RRSIG    NSEC 5 3 81400 20101202201350 (       20101102201350 42199 brytec.com.br.
                                                        HJgOld3zjnowD/bK6uh/SbiOp+RQBrzTQpL2
                                                        IwYGbO6icsBgjjnkCJAUIrTDNCXx0EB+TgFX
                                                        TnL8fgtLqikGbExLnu7mEI3pbX0MdSi48uWn
                                                        jbi8tzQJr5NX5q2fpZOoeaQjX/hpirPl9aD3
                                                        545YPHkXIkapE2dPDNG2LEoyw2c= )

3600    DNSKEY    257 3 5 (                           AwEAAePpkLBaYj+NzSo388VFAEd+YjfRUixm
                                                        4Zn4vJkPnPrkqWPeeCRs+eX5UGucxUtEDag7
                                                        PDkC9hadMvAdHQbMtt8JS2sriE75BcLNCaJ+
                                                        lkOelqk16oCQEcpzpQ5Nh+vmoqJfiMYTlwwB
                                                        3MdSwdTpsdWhEtziHOCK1tU8xCa9foA7
                                                        ) ; key id = 42199

3600    RRSIG    DNSKEY 5 3 3600 20101202201350 (       20101102201350 42199 brytec.com.br.
                                                        qWR3ZSqNsX3Z5bTDFMFelCGD8ClUz+3OlEQ0
                                                        25aa1COLrGglJb8UVnTHqxsOQmHc4h/NUqRy
                                                        mjzSQe4fJJB9XhGEeAwZ5HkOdjIEXvEcJyHy
                                                        GgmJPYjWY7RJMZOrrNL+FTDgiMxPXua+XGjL
                                                        wi6R/G7ry6T8PA/u1RizeePqYq8= )
```

Figura 21: Arquivo de zona assinado.

Figura 22: Sistema de provisionamento do registro.br.

```
$ cat dsset-brytec.com.br.

brytec.com.br. IN DS 42199 5 1        2697F78121A4735C2F36667C48322D14960112B6
brytec.com.br. IN DS 42199 5 2        61814A1AB2E65FF098A56C61DC00E9F7A65DAC9A5153738C6266A899 3B90FCC2
```

Figura 23: Arquivo DS gerado.

Os paramêtros utilizados com o DIG foram os seguintes:

- +dnssec: requisição DNSSEC;
- +multiline: imprime os dados com identação;
- +noadditional: não exibe informações adicionais.

A primeira figura demonstra a utilização do DIG apontando para o domínio *ufsc.br* que não possui DNSSEC.

```
$ diq @150.162.1.3 ufsc.br +dnssec +multiline +noadditional
;; ANSWER SECTION:
ufsc.br.          3 IN A  150.162.1.152
ufsc.br.          3 IN A  150.162.1.9

;; AUTHORITY SECTION:
ufsc.br.          43200 IN NS ciasc-gw.ciasc.gov.br.
ufsc.br.          43200 IN NS ns.ufsc.br.
ufsc.br.          43200 IN NS ns3.ufsc.br.
ufsc.br.          43200 IN NS ns.pop-sc.rnp.br.

;; Query time: 31 msec
;; SERVER: 150.162.1.3#53(150.162.1.3)
;; WHEN: Tue Nov 02 22:52:35 2010
;; MSG SIZE  rcvd: 224
```

Figura 24: Consulta ao DNS da ufsc.br.

A segunda figura mostra a requisição DNS do domínio *brytec.com.br* que utiliza DNSSEC. Percebe-se a presença dos registros RR SIG contendo a assinatura e evidenciando a utilização do DNSSEC.

7.4 Conclusão

O objetivo primordial das configurações acima relatadas era a implementação do DNSSEC no ambiente. Após as demonstrações práticas expostas, com os dados apresentados e de acordo com requisição DNS ao domínio *brytec.com.br* pode-se identificar o pleno funcionamento do DNSSEC atingindo-se, portanto, o objetivo inicial proposto.

```
dig @201.2.240.6 brytec.com.br soa +dnssec +multiline +noadditional
;; ANSWER SECTION:
brytec.com.br.        3600 IN SOA dns.brytec.com.br. root.brytec.com.br. (
                      2010110102 ; serial
                      3600       ; refresh (1 hour)
                      900        ; retry (15 minutes)
                      604800     ; expire (1 week)
                      86400      ; minimum (1 day)
                      )
brytec.com.br.        3600 IN RRSIG SOA 5 3 3600 20101201183619 (
                      20101101183619 34558 brytec.com.br.
                      AU8+eatvApDG/y1l3yEfdbp6sLeAaSbfCUUMTpXNTJRB
                      LSBt7fN3/rSpIOQjbiShWRKlBp3zhnEfGd5N/+6iP/LO
                      tWy8Nq0YJIVeXrgmwwtbQFZ2G4TdWJofBsC5twMicZEC
                      C/ZADJis2Fmt6qIDF6JV7vtM6VkOSwFcxcPq/Zs= )

;; AUTHORITY SECTION:
brytec.com.br.        86400 IN NS dns.brytec.com.br.
brytec.com.br.        86400 IN RRSIG NS 5 3 86400 20101201183619 (
                      20101101183619 34558 brytec.com.br.
                      d5RGGPpzjBdUxyZwgfW7iVrQPZzmhXLS1qYlQJ1o72Av
                      wCbzYs3mHjIQnVnmxPVyVWDCu93zxBWaaeKu3XHBVQZZ
                      EviEnizRkRQRM42gJQk+PlqNS4PH5JTyb1k1rXWyzxhR
                      uSb+vd0RnAGyNpTPBhuJkHaxNlaWoRqpue4EP9w= )
```

Figura 25: Consulta ao DNS da brytec.com.br.

8 Conclusão

Atualmente, o uso do DNS para a resolução de nomes de domínio ainda é muito utilizado apesar da comprovada falta de segurança. Um dos principais fatores dessa insegurança é a possibilidade de um atacante poluir o conteúdo do cachê dos servidores DNS através de um ataque *Man in the middle*.

Neste cenário, as extensões de segurança providas pelo DNSSEC se mostram competentes para ajudar na solução de parte dos problemas encontrados. Com tecnologias bastante difundidas e comprovadamente eficientes como o uso de criptografia de chaves públicas e assinaturas digitais, o DNSSEC vem se mostrando um padrão na Internet e sua adoção, por parte dos administradores de rede, se mostra quase uma obrigação.

Fica evidente que o uso de outras tecnologias de segurança, trabalhando em conjunto com o DNSSEC, ajudam a tornar a rede de computadores mais segura. Uma dessas tecnologias abordada neste trabalho é o SSL, que pode ser utilizado para garantir um canal de segurança entre o cliente e o servidor.

Através da confecção deste trabalho e do levantamento bibliográfico sobre os assuntos do enrredo, foi possível observar mediante detalhamentos das RFC citadas, que o uso do DNSSEC é indicado para solucionar ou atenuar grande parte dos problemas de segurança encontrados na resolução de nomes na Internet.

Dessa maneira, o uso de servidores de nomes com a tecnologia DNSSEC podem garantir que os dados foram emitidos por quem realmente se espera e não por alguém tentando se passar pelo servidor original, sendo esta a solução para o grande problema de segurança da resolução de nomes, a poluição de cachê.

9 Trabalhos Futuros

Este trabalho pode ser interpretado como um documento introdutório ao DNSSEC e aos assuntos que lhe cercam. Vários temas e assuntos necessários para um profundo entendimento não foram abordados ou não receberam a devida atenção, sendo este documento apenas o primeiro de uma série de trabalhos que podem ser criados. Desta maneira, entende-se que muita pesquisa e levantamento bibliográfico ainda são necessários.

Dentre os trabalhos futuros identificados destacam-se:

- Execução e demonstração de um ataque ao DNS e DNSSEC com apresentação dos resultados.
- Análise comparativa de desempenho entre servidores DNS e DNSSEC medindo o impacto dos mecanismos de segurança.
- Estudo e pesquisa de outras abordagens e novos ataques desenvolvidos contra o DNSSEC.
- Pesquisa e implementação de mecanismos de segurança que garantam proteção contra ataques de negação de serviço.
- Comparação do DNSSEC com outras soluções que visam garantir a segurança na resolução de nomes.

Apêndice A - Roteiro de Instalação

Os roteiros de configurações, aqui expostos, se referem ao software BIND e se baseam em tutorias oficiais disponibilizados pelo Registro.br e podem ser encontrados em [42].

A figura abaixo ilustra o cenário hipotético que será considerado no roteiro de instalação.

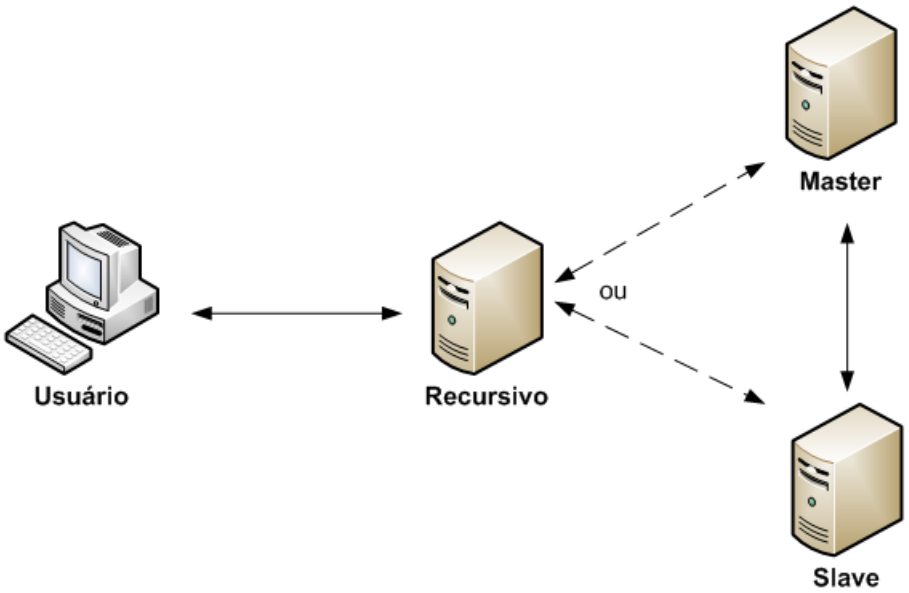

Figura 26: Cenário hipotético - instalação DNSSEC

Configuração de um Servidor Autoritativo

- Verificar a disponibilidade do domínio junto ao Registro.br;
- Instalar o BIND (disponível em http://www.isc.org/) nos servidores;
- Configurar os arquivos de zona e *named.conf* no servidor *Master* e *named.conf* no servidor *Slave*;
- Executar o BIND nos servidores;
- Atualizar o registro do domínio (com os regisros NS) e aguardar publicação;

Arquivo de Zona

```
foo.eng.br. IN SOA ns1.foo.eng.br. hostmaster.foo.eng.br. (
        1 ; serial
        3600 ; refresh
        3600 ; retry
        3600 ; expire
        900 ) ; TTL
foo.eng.br. IN NS ns1.foo.eng.br.
foo.eng.br. IN NS ns2.foo.eng.br.
exemplo.foo.eng.br. IN NS ns2.exemplo.foo.eng.br.
exemplo.foo.eng.br. IN NS ns1.exemplo.foo.eng.br.
ns1.foo.eng.br. IN A 200.160.3.97
ns2.foo.eng.br. IN A 200.160.10.251
ns1.exemplo.foo.eng.br. IN A 200.160.3.97
ns2.exemplo.foo.eng.br. IN A 200.160.10.251
```

named.conf

```
options {
        directory "/etc/namedb";
        pid-file "/var/run/named/pid";
        dump-file "/var/dump/named dump.db";
        statistics-file "/var/stats/named.stats";
        listen-on { 200.160.10.251; };
};

{;
zone "foo.eng.br" {
        type master;
        file "/etc/namedb/db.foo";
        allow-transfer {
                200.160.3.97;
        };
};
zone "exemplo.foo.eng.br" {
        type master;
        file "/etc/namedb/db.exemplo.foo";
        allow-transfer {
                200.160.3.97;
        };
};
```

Figura 27: Exemplos de um arquivo de zona e do arquivo named.conf

- Realizar testes no servidor (DIG);
- Criar a chave com o comando *dnssec-keygen*;
- Incluir a chave no arquivo de zona ($include)
- Assinar a zona com o comando *dnssec-signzone*;
- Atualizar o arquivo *named.conf* do servidor *Master* para utilizar o arquivo de zona assinado;
- Restartar o BIND no servidor *Master*;
- Adicionar na interface de provisionamento, no Registro.br, o DS (localizado no arquivo *dsset*);
- Aguardar nova publicação.

Configuração de um Servidor Recursivo

- Instalar a biblioteca OpenSSL (disponível em *http://www.openssl.org/*);
- Instalar o BIND (disponível em http://www.isc.org/)

- Obter a *trusted-key* do site do Registro.br;
- Incluir a *trusted-key* no arquivo named.conf;

```
options {
        directory "/etc/namedb";
        pid-file "/var/run/named/pid";
        dump-file "/var/dump/named dump.db";
        statistics-file "/var/stats/named.stats";
        dnssec-enable yes;
        dnssec-validation yes;
        listen-on {
                200.160.3.102;
        };
};
trusted-keys {
        br. 257 3 5
                "AwEAAa290pX9aaNf053wZdkOGKmNCbLlbyCo1yNrwDiv
                fgyBcdT+cjtVwSEmzh6HoY+lQeJKJDpbJF1/G9ZbA/Aw
                rKCpahLFDz5SaZiP0sStuWg8UzWz8b5J5t2dlxsu6PeF
                dU08fkItt1FDEGCxsy3IR+eYJGdK0jowuDySoiQ8Uj/+
                3ZHM4I4z2gOzEwb8uI3Jntmj5azop4B2o1WDNV1VdPJl
                96TvMy5ImGsBkn03y3FUrQpynQn8M2x5pztuGEOg8KP2
                Yp/VUp0V0HyqTjSPsM+mCT2x80xN5SghaMeby85u5fVs
                OEks3T6fN27nFxrdnMvcmNlslwcQvbxWSwTNVeU=";
};
```

Figura 28: Exemplo de inclusão de chave.conf

- Executar o BIND;

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 com o DIG.

Referências

[1] A. S. Tanenbaum. *Redes de Computadores, 4ª Edição.* [S.l.]: Campus, 2003.

[2] Douglas E. Comer. *Redes de Computadores e Internet.* [S.l.]: Bookman, 2001.

[3] M. A. Thompson. *Proteção e Segurança na Internet.* [S.l.]: Érica, 2002.

[4] William Stallings. *Cryptography and Network Security: Principles and Practice.* [S.l.]: Prentice Hall, 2003.

[5] Daniel Balparda de Carvalho. *Segurança de Dados com Criptografia: Métodos e Algorítmos.* [S.l.]: Book Express, 2000.

[6] D. R. Stinson. *Cryptography: Theory and Practice.* [S.l.]: CRC Press, 1995.

[7] Marcelo Luiz Brocardo; Carlos Roberto De Rolt; Reinaldo Fernandes. *Introdução à Certificação Digital - Da Criptografia ao Carimbo do Tempo.* [S.l.]: Editora BRy Tecnologia, 2003.

[8] W. Diffie; M. Hellman. *New Direction in Criptography.* [S.l.], 1976.

[9] W. Stallings. *Redes de Computadores.* [S.l.]: Campus, 2005.

[10] Luciano Siqueira. *LPI Nível2: Aula 11.* [S.l.]: Revista Linux Magazine, 2008.

[11] S. Northcutt. *Segurança e Prevenção em Redes.* [S.l.]: Berkeley, 2001.

[12] Evi Nemeth; Garth Snyder; Trent R. Hein. *Manual Completo do DNS.* [S.l.]: Books, 2004.

[13] Rede Nacional de Ensino e Pesquisa da Bahia. *DNSSEC: adicionando mais segurança no Sistema de Nomes de Domínio.* 2010. URL: http://www.pop-ba.rnp.br/cert/DNS_SECDocDetalhada.

[14] RNP - Rede Nacional de Ensino e Pesquisa. *Boletim bimestral sobre tecnologia de redes de computadores.* 1998. URL: http://www.rnp.br/newsgen/9801/dnssec.html.

[15] Network Working Group. *Protocol Modifications for the DNS Security Extensions.* 2005. URL: http://tools.ietf.org/html/rfc4035.

[16] Network Working Group. *DNS Security (DNSSEC) NextSECure (NSEC) RDATA Format.* 2001. URL: http://tools.ietf.org/html/rfc3845.

[17] George Luiz Cardoso Buriti. *Extensões de Segurança para o DNS.* [S.l.], 2006.

[18] Network Working Group. *Resource Records for the DNS Security Extensions.* 2005. URL: http://tools.ietf.org/html/rfc4034.

[19] Network Working Group. *Clarifications to the DNS Specification*. 1997. URL: http://tools.ietf.org/html/rfc4035.

[20] Network Working Group. *Site Security Handbook*. 1997. URL: http://tools.ietf.org/html/rfc2196.

[21] British Standards Institution. *BS 7799*. 2002. URL: http://www.induction.to/bs7799/.

[22] International Standartization Organization; International Engineering Consortium. *NBR ISO/IEC 17799*. [S.l.], 2007.

[23] Mark Crosbie. *Intrusion Detection Pages*. 2001. URL: http://www.cerias.purdue.edu/coast/intrusiondetection/welcome.html.

[24] Frank Ned. *Ferramentas IDS*. 1999. URL: http://www.revista.unicamp.br/infotec/artigos/frank4

[25] Marcos Antonio Popper; Juliano Tonizetti Brignoli. *Engenharia Social - Um Perigo Eminente*. [S.l.], 2003.

[26] Kevin D. Nitnick; William L. Simon. *A Arte de Enganar*. [S.l.]: Pearson, 2003.

[27] Denise Ranghetti Pilar da Silva; Lilian Milnitsky Stein. *Segurança da informação: uma reflexão sobre o componente humano*. [S.l.], 2007.

[28] Gleydson Mazioli da Silva. *Guia Foca GNU/Linux*. [S.l.], 2007.

[29] P. G. Neumann. *Inside Denial-of-Service Attacks*. [S.l.], 2000.

[30] Howard Eland. *Política de Segurança da Informação para Redes Corporativas*. [S.l.], 2006.

[31] Timothy R. Schmoyer; Yu Xi Lim; Henry L. Owen. *Wireless Intrusion Detection and Response: A Case Study Using the Classic Man in the Middle Attack*. [S.l.], 2004.

[32] MEN and MICE. *What is DNS Spoofing*. 1999. URL: http://www.menandmice.com/.

[33] Sacramento et al. *Relatório Técnico - Provendo Segurança na Resolução de Nomes do DNS*. [S.l.], 2001.

[34] Jairo Ferraz. *Redes II : Aula - Firewall parte 2 - Faculdade Paraíso - CE*. 2010. URL: http://jairoferraz.com/aulas/redes2/Firewall2.pdf.

[35] Vagner Sacramento; Cláudio Monteiro. *Falsificação de endereços IP: Um Perigo que Ronda os Serviços de Resolução de Nomes na Internet*. [S.l.], 2000.

[36] Artur Gustavo Alves Gomes; Luiz Tomé de Farias Neto. [S.l.].

[37] Everton Schonarie Pasqual. *IDDE - Uma Infra-estrutura para a Datação de Documentos Eletrônicos*. [S.l.], 2001.

[38] Steve Friedl. *An Illustrated Guide to the Kaminsky DNS Vulnerability*. 2008. URL: http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html.

[39] Network Working Group. *Domain Name System Security Extensions*. 1997. URL: http://tools.ietf.org/html/rfc2065.

[40] David Robert Camargo de Campos; Rafael Dantas Justo. *Tutorial DNSSEC*. 2010. URL: ftp://ftp.registro.br/pub/doc/tutorial-dnssec.pdf.

[41] Howard Eland. *Securing a Domain: SSL vs. DNSSEC*. [S.l.], 2009.

[42] Registro.br. *Tutoriais - DNS e DNSSEC*. 2010. URL: http://registro.br/suporte/tutoriais/dnssec.html.