Implementando o DNSSec na prática

Dioni da Rosa[1], Roberto Franciscatto[1], Maurício Sulzbach[2]

[1] Departamento Graduação, Pós-Graduação e Pesquisa – Colégio Agrícola de Frederico Westphalen (CAFW)
Universidade Federal de Santa Maria (UFSM)
98400-000 – Frederico Westphalen – RS – Brasil

[2] Departamento de Engenharia e Ciência da Computação - Universidade Regional Integrada do Alto Uruguai e das Missões (URI)
Frederico Westphalen – RS – Brasil

dionitei@hotmail.com, roberto@cafw.ufsm.br, sulzbach@uri.edu.br

Abstract. *This article aims to describe the concepts that encompass the use of DNSSec this that presents itself as an extension of the protocol secure DNS (Domain Name System), which is essential for using the internet, allowing the location and of domains names solution into IP addresses. In this sense, this article seeks to understand the use of DNSSec improve the security of the network used in the same.*

Resumo. *O presente artigo tem como objetivo descrever os conceitos que englobam a utilização do DNSSec, este que apresenta-se como uma extensão segura do protocolo DNS (Domain Name System), que é fundamental para utilização da internet, permitindo a localização e solução dos nomes de domínios em endereços IPs. Nesse sentido, tal artigo busca compreender a utilização do DNSSec no aperfeiçoamento da segurança da rede empregada no mesmo.*

1. Introdução

A abordagem deste trabalho irá basear-se na descrição do DNSSec (*Domain Name System Security Extensions*), tratando da segurança de redes, aspecto importante e fundamental nos serviços de internet. O DNSSec tem em sua base a utilização de tecnologias de criptografia de chaves públicas e privadas, desta forma, fornece a integridade dos dados e autenticação para resolver problemas de segurança e aplicações através da a utilização de assinaturas digitais criptográficas.

O presente artigo está organizado da seguinte forma: na seção 2, é apresentada uma base teórica/descritiva sobre o funcionamento geral do DNS; na seção 3 é apresentado o DNSSec e sua forma de funcionamento; na seção 4 é apresentado um breve comparativo entre o serviço de DNS convencional e o DNSSec; e por fim na seção 5 são apresentadas as conclusões geradas na investigação deste trabalho.

2. Compreendendo o DNS

O Sistema de Nomes de Domínio (DNS - *Domain Name System*) é um banco de dados distribuído. Isso permite um controle local dos segmentos do banco de dados global, embora os dados em cada segmento estejam disponíveis em toda a rede através de um esquema cliente-servidor [Microsoft, 2013]. O DNS possui arquitetura hierárquica,

uma distribuição eficiente, descentralizada e com cache, conforme ilustrado na Figura 1.

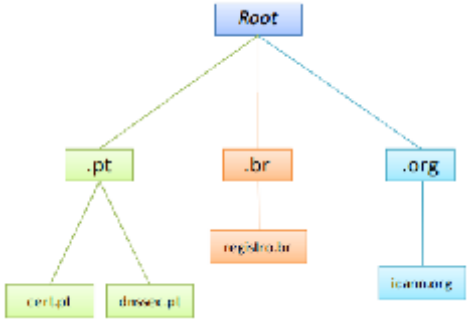

Figura 41. Cadeia de domínios - Fonte: Cert.pt(2013)

O principal propósito do DNS é a resolução de nomes de domínio em endereços IP e vice-versa como: **site.com.br** em **200.160.10.251.** A entidade responsável por gerenciar os endereços e números IPs é a ICANN (Corporação da Internet para Atribuição de Nomes e Números), uma entidade sem fins lucrativos que tenta manter todos os sites registrados funcionando na internet [Cert PT, 2013].

3. DNSSec

Pode-se compreender o DNSSec como uma extensão que faz uso de criptografia assimétrica para garantir a autenticidade e a integridade da informação transmitida entre servidores DNS e aplicações do utilizador, ou seja, o DNSSec é uma extensão de segurança do protocolo DNS [RNP, 2013]. Ao mesmo tempo em que é uma extensão do DNS, o funcionamento dos mecanismos de segurança previstos no DNSSec complementam e são transparentes para o utilizador, sendo que não interferem no normal funcionamento do protocolo DNS.

A segurança implantada no DNSSec se baseia na criptografia assimétrica com um par de chaves distintas, mas relacionadas entre si, definidas como chave pública e chave privada [Cert Bahia, 2013]. Em termos técnicos as principais responsabilidades em relação à utilização de criptografia assimétrica no DNSSEC são:

- Delimitação rigorosa das chaves privadas aos legítimos detentores;
- Distribuição fidedigna de chaves públicas a todos os que delas necessitem;
- Atualização da informação da assinatura da zona com a hierarquia superior;
- Correta manutenção da zona assinada;
- Gestão do tempo de vida dos pares de chaves.

3.1 Configuração do DNSSec em um domínio

Para validar um domínio através do DNSSec, deve-se começar com a criação de chaves utilizando o comando *dnssec-keygen* (neste exemplo, considerando um sistema operacional linux, executando o serviço de DNS *Bind*, sendo todas as operações realizadas no servidor principal - Master), que irá gerar dois arquivos com extensão *.key* e *.private*. Posteriormente, o comando *dnssec-signzone* é utilizado para assinar o domínio; este comando irá gerar o arquivo de zona com a extensão *.signed*, contendo uma assinatura que possui um período de validade padrão de 30 dias, podendo ser modificado. Em seguida, deve-se atualizar as configurações do arquivo *named.conf*, arquivo este que contém uma coleção de declarações e entre elas o caminho do arquivo

de zona do domínio, e então reiniciar o *Bind*[15] [Kuroiwa, 2013]. Por fim, deve-se copiar os dados presentes nos campos *KeyTag* e *Digest* do arquivo *dsset-dominio.com.br*, para a interface no site http://registro.br. A Figura 2 ilustra os comandos para geração de chaves, arquivo de zona, atualização do *named.conf*, extração de dados do arquivo ds-set, bem como, publicação no Registro.br.

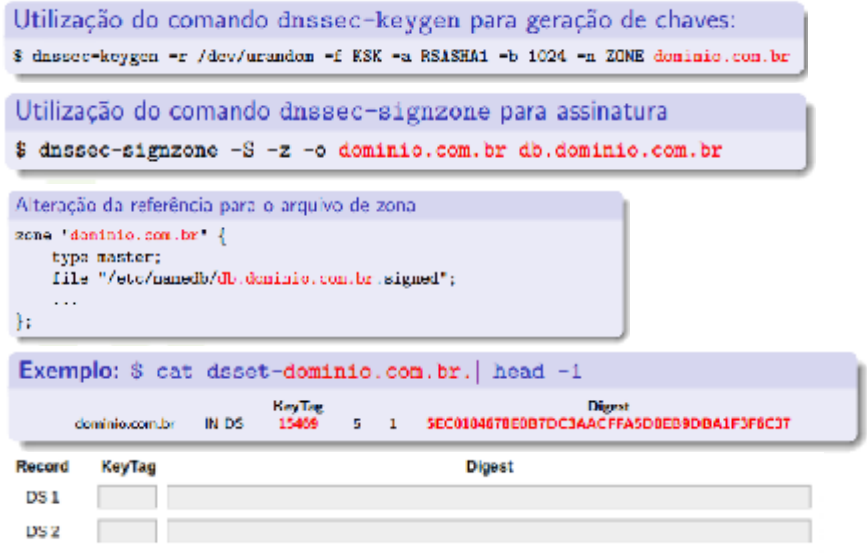

Figura 42. Configurações para habilitar DNSSec em um domínio - Fonte: Kuroiwa(2013)

4. DNS x DNSSec

A demonstração de como trabalha o DNS em comparação com o DNSSec está ilustrado na Figura 3, no qual se tem o sistema de resolução de nomes mais seguro, reduzindo o risco de manipulação de dados e domínios forjados [Kuroiwa, 2013]. O mecanismo utilizado pelo DNSSec é baseado na tecnologia de criptografia que emprega assinaturas.

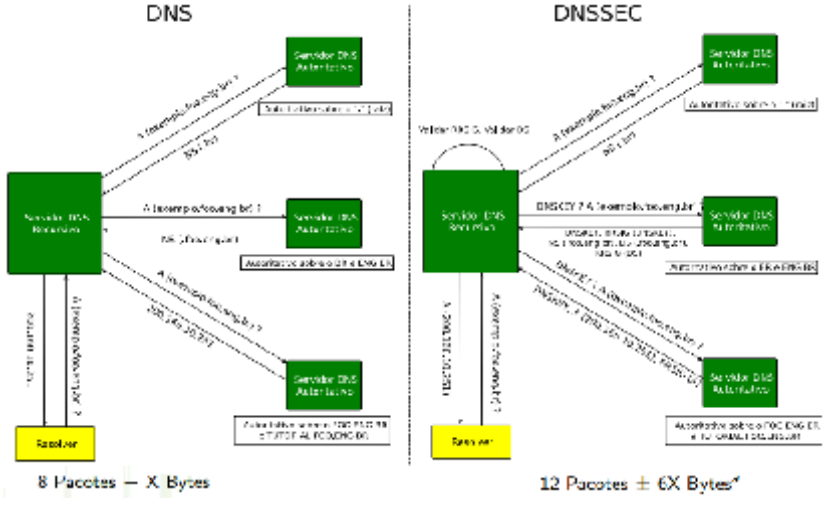

Figura 43. Comparação DNS x DNSSec - Fonte: Kuroiwa(2013)

[15] BIND (Berkeley Internet Name Domain) é o servidor para o protocolo DNS.

O DNSSec soluciona alguns problemas encontrados no DNS quanto a implementação de segurança, pois falsas informações DNS criam oportunidades para roubo de informações de terceiros ou alteração de dados em diversos tipos de transações, como compras eletrônicas. Na tecnologia DNS, um ataque com informação forjada é extremamente difícil de ser detectado e na pratica impossível de ser prevenido. O objetivo da extensão DNSSec é assegurar o conteúdo do DNS e impedir estes ataques validando os dados e garantindo a origem das informações, pois como é apresentado na Figura 3 as requisições passam por uma validação de chave, caso a chave seja invalida a requisição é encerrada, impedindo assim os domínios forjados para fraudes. Além disso, a não utilização do DNSSec pode acarretar uma série de outras vulnerabilidades como: poluição de cache, updates não autorizados, dados corrompidos, entre outros.

5. Conclusão

Entende-se através deste trabalho que a utilização do DNSsec em um domínio é fundamental para evitar problemas relativos as vulnerabilidades conhecidas do DNS, bem como, assegurar que determinados serviços que dependem de um nível de segurança apropriado possam efetivamente estar o maior tempo possível disponível e de forma estável.

Por fazer uso de chaves assimétricas (publicas e privadas) o DNSSec garante a integridade e originalidade dos dados que são transmitidos através deste protocolo, pois os dados são validados quando recebidos através de uma chave, o que impossibilita a alteração dos dados entre o ponto de transmissão e recepção. Desta forma se torna correto afirmar que a utilização do DNSSec bem implementado consente segurança aos dados transmitidos em relação ao DNS sem a implementação de criptografia.

Referências

Cert Bahia. (2013) "DNSSEC: Adicionando mais segurança no Sistema de Nomes de Domínio", http://www.pop-ba.rnp.br/Cert/DNSSEC_DocDetalhada#Uso_de_criptografia_assim_trica, Setembro.

Cert PT. (2013) "Boas Praticas de Segurança", http://www.dnssec.pt/docs_pt/DNS-Boas_Praticas_Seguranca_v6.pdf, Maio.

Kuroiwa, C. H. (2013) "Tutorial DNSSEC", ftp.registro.br/pub/doc/tutorial-dnssec.pdf, Setembro.

Microsoft. (2013) "Função Servidor DNS", http://technet.microsoft.com/pt-br/library/cc753635(v=ws.10).aspx, Setembro.

RNP. (2013) "DNSSEC: O Que É e Por Que Precisamos Dele", http://www.rnp.br/newsgen/9801/dnssec.html, Setembro.