Universidade de Lisboa
Faculdade de Ciências
Departamento de Informática

ESTUDO E REALIZAÇÃO DE UMA INSTALAÇÃO PILOTO DE DNSSEC PARA O DNS DE .PT

Sara Cristina da Silva Monteiro

Mestrado em Engenharia Informática

2007

Universidade de Lisboa
Faculdade de Ciências
Departamento de Informática

ESTUDO E REALIZAÇÃO DE UMA INSTALAÇÃO PILOTO DE DNSSEC PARA O DNS DE .PT

Sara Cristina da Silva Monteiro

Projecto orientado pelo Prof. Dr. Miguel Pupo Correia
e co-orientado por Dr^a Luísa Gueifão

Mestrado em Engenharia Informática

2007

Declaração

Sara Cristina da Silva Monteiro, aluna nº 29264 da Faculdade de Ciências da Universidade de Lisboa, declara ceder os seus direitos de cópia sobre o seu Relatório de Projecto em Engenharia Informática, intitulado "Estudo e realização de uma instalação piloto de DNSSEC para o DNS de .PT" , realizado no ano lectivo de 2006/2007 à Faculdade de Ciências da Universidade de Lisboa para o efeito de arquivo e consulta nas suas bibliotecas e publicação do mesmo em formato electrónico na Internet.

FCUL, 31 de Agosto de 2007

Luísa Lopes Gueifão, supervisora do projecto de *Sara Cristina da Silva Monteiro*, aluna da Faculdade de Ciências da Universidade de Lisboa, declara concordar com a divulgação do Relatório do Projecto em Engenharia Informática, intitulado "Estudo e realização de uma instalação piloto de DNSSEC para o DNS de .PT".

Lisboa, 31 de Agosto de 2007

Resumo

O DNS (Domain Name System - Sistema de Nomes de Domínios) é uma das ferramentas fundamentais para o funcionamento da Internet que permite localizar e resolver nomes de domínio em endereços IP e vice-versa.

Com o crescimento da Internet e do número de utilizadores os perigos e a necessidade para a consciencialização da segurança aumentaram, revelando-se de extrema importância a procura de soluções que garantam um ambiente mais seguro no serviço e na rede.

Nesse sentido desenvolveu-se internacionalmente o DNSSEC, um conjunto de extensões realizadas ao protocolo DNS que permitem a verificação da autenticidade e integridade dos dados e com o qual se pretende proteger a Internet e os seus utilizadores de determinado tipo de ataques.

Este projecto aborda o processo de análise e integração das extensões de segurança ao protocolo DNS no serviço de registo de domínios sob a designação .PT, prestado pela FCCN, com vista a alcançar melhorias de segurança a nível da rede nacional e contribuindo para tornar a Internet mais segura a nível global.

Abstract

In order to access Internet resources using the user-friendly domain names rather than IP addresses, users need a system to translate domain names into IP addresses. This translation is the primary task of the Domain Name System (DNS).

The Internet is the world's largest computing network, with hundreds of million of users. As this community grows there is a need to be aware of threats and dangers and to find solutions for secure service and network environments.

In that sense, a community of Internet developers designed DNSSEC, a set of extensions to the DNS system to prevent some types of attacks against it, performing source authentication of domain name information and maintaining data integrity.

This project focus on the process of analysis and integration of the DNSSEC extensions in the .PT domain name service, handled by FCCN, in order to reach some security improvements in the national network and to give some contribution to a more secure world wide Internet.

Conteúdo

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

Este documento descreve o projecto realizado no âmbito da disciplina Projecto em Engenharia Informática (PEI[1]) do Mestrado em Engenharia Informática da Faculdade de Ciências da Universidade de Lisboa.

Num mundo de comunicação global e distribuída, é fundamental que os sistemas informáticos utilizados ofereçam cada vez mais garantias de segurança.

O projecto aborda a problemática da falta de segurança na utilização do serviço de nomes de domínio (DNS) [1]. É apresentada uma solução a algumas das vulnerabilidades no sistema existente, utilizando a implementação de extensões de segurança ao DNS, DNSSEC [2].

O DNS não foi originariamente desenhado com preocupações de segurança, mas perante a crescente importância da informação que este serviço fornece, tornou-se importante ao longo do percurso de expansão da Internet assegurar a comunicação entre os sistemas informáticos.

O DNSSEC consiste num conjunto de normas internacionais que extendem a tecnologia DNS, fornecendo integridade e autenticação dos dados, com suporte a respostas assinadas criptograficamente.

Este trabalho tem como objectivo melhorar a segurança do DNS do serviço de registo de domínios .PT [3] através da implementação do DNSSEC.

1.1 Enquadramento Institucional

A FCCN [4] é uma instituição privada sem fins lucrativos designada de utilidade pública que iniciou a sua actividade em Janeiro de 1987. Desde então, com o apoio das Universidades e diversas instituições de I&D nacionais, a FCCN tem contribuído para a expansão da Internet em Portugal.

[1] http://www.di.fc.ul.pt/disciplinas/pei/pei0607/

Como principal actividade a FCCN tem o planeamento, gestão e operação da Rede Ciência, Tecnologia e Sociedade (RCTS), uma rede de alto desempenho para fins de investigação e ensino nacional, constituindo-se assim uma plataforma de experimentação para aplicações e serviços avançados de comunicações.

A RCTS é uma rede informática que usa os protocolos da Internet para garantir uma plataforma de comunicação e colaboração entre as instituições do sistema de ensino, ciência, tecnologia e cultura.

B-ON - Biblioteca Científica Nacional, E-U - Campus Virtual, 6Net e mais recentemente o Portal Internet Segura, são muitos dos inúmeros projectos desenvolvidos pela FCCN.

À FCCN, foi ainda delegada pela *IANA - Internet Assigned Numbers Authority*, organização depois substituída pelo *ICANN - Internet Corporation for Assigned Names and Numbers*, a responsabilidade pela gestão do ccTLD (country code Top Level Domain) .PT, o serviço de registo de domínios sob o domínio nacional .PT.

A nível internacional, a FCCN tem vindo a participar activamente, na qualidade de membro e de interveniente, em reuniões e grupos de trabalho de organizações credenciadas no âmbito da Internet como o ICANN e o *CENTR - Council of European National Top level domain Registries*.

No âmbito das recomendações emanadas por estas entidades, a FCCN pretende desenvolver trabalho no sentido de garantir tecnicamente, entre outros aspectos:

- A gestão técnica e administrativa do espaço de endereços Internet sob .PT;
- A correcta configuração e operação do servidor primário da zona DNS PT;
- A manutenção de uma base de dados dos domínios registados, acessível via Internet;
- A disponibilização de dados estatísticos sobre o registo de domínios de .PT;
- A avaliação do serviço prestado à comunidade.

O Serviço DNS de .PT consiste num serviço autónomo no âmbito das actividades da FCCN e tem no seu grupo uma área técnica de suporte ao seu trabalho de sistema de nomes de domínios de .PT.

Enquadrado neste grupo, este estágio consistiu numa primeira fase de cerca de 4 meses, no conhecimento dos diversos projectos da FCCN e no acompanhamento do trabalho do DNS de .PT, sendo posteriormente dedicado exclusivamente a este projecto.

Atento o facto do DNS ser o sistema de atribuição de endereços IP a nomes de domínios, desde logo se tornou evidente e motivador o desenvolvimento deste trabalho quer pela sua componente técnica quer pelo impacto positivo e alargado que o funcionamento real de uma implementação de DNSSEC potencia e garante.

1.2 Organização do documento

O relatório encontra-se organizado da seguinte forma:

- Capítulo 2 - "Objectivos" - apresenta os objectivos do projecto, o contexto subjacente, a metodologia utilizada e o planeamento realizado para o concretizar.
- Capítulo 3 - "Trabalho Realizado" - apresenta concretamente o que se fez e as ferramentas utilizadas. São aqui também apresentadas as possiblidades de trabalho futuro e os possíveis métodos de integração das extensões de segurança ao sistema actual.
- Capítulo 4 - "Sumário e Conclusões" - apresenta um sumário do trabalho realizado, o que ainda está por realizar e as conclusões tiradas com a realização do projecto.

Capítulo 2

Objectivos

Este capítulo introduz o contexto em que o projecto se enquadra, os conceitos importantes para a compreensão do trabalho realizado, os objectivos e a motivação que levou à concretização deste trabalho. Apresenta também alguns trabalhos relacionados, com grande relevância no âmbito em que se insere este projecto.

Por fim, é apresentada uma secção com a metodologia seguida no desenvolvimento do projecto bem como o planeamento efectuado para o concretizar.

2.1 Âmbito do projecto

2.1.1 Domain Name Service

A Internet existe desde que o protocolo TCP/IP (Transmission Control Protocol/Internet Protocol) foi desenvolvido no início dos anos 70. Tornou-se rapidamente o protocolo padrão de rede no ARPANET. Desde então a rede tem crescido de centenas para milhões de utilizadores.

Desde cedo que os computadores ligados entre si em rede tiveram a necessidade de sistemas que os permitissem identificarem-se rapidamente, para tal, todos os computadores passaram a ter um nome associado. Esses nomes na Internet no entanto eram inicialmente incluídos num único ficheiro designado "hosts.txt"que tinha de ser instalado em todos os computadores que faziam parte da rede.

O Stanford Research Institute Network Information Center (SRI-NIC) tornou-se na autoridade responsável por gerir e distribuir esse ficheiro. Mais tarde, a necessidade de um único domínio para cada computador e um espaço de nomes hierárquico preparou o lançamento de um novo protocolo de rede que viria preencher todos os requisitos da Internet em crescente expansão.

Em adição ao TCP/IP, dois grandes protocolos foram desenhados nos anos 80 para permitir que o crescimento da rede ocorresse com maior facilidade. Estes protocolos são o DNS (Domain Name Service) e BGP (Border Gateway Protocol). Juntos, estes três protocolos compoêm o núcleo de infrastrutura da Internet.

P. Mockpetris desenhou o sistema de serviço de nomes de domínios (DNS) com vista à estabilidade e robustez mas sem preocupações de segurança [1]. A nova ideia surgiu por forma a não haver uma única entidade responsável pelo ficheiro de nomes mas sim uma imensidade de entidades.

O novo sistema DNS, baseado no conceito de descentralização, tem três grandes componentes: a base de dados; o servidor; e o cliente. A base de dados é distribuída e contém os resource records (RRs) dos domínios que definem a zonas de domínios numa árvore DNS, como a apresentada na Figura 2.1. Estes RRs são registos de recurso que delegam a autoridade de configuração de uma zona a uma determinada entidade.

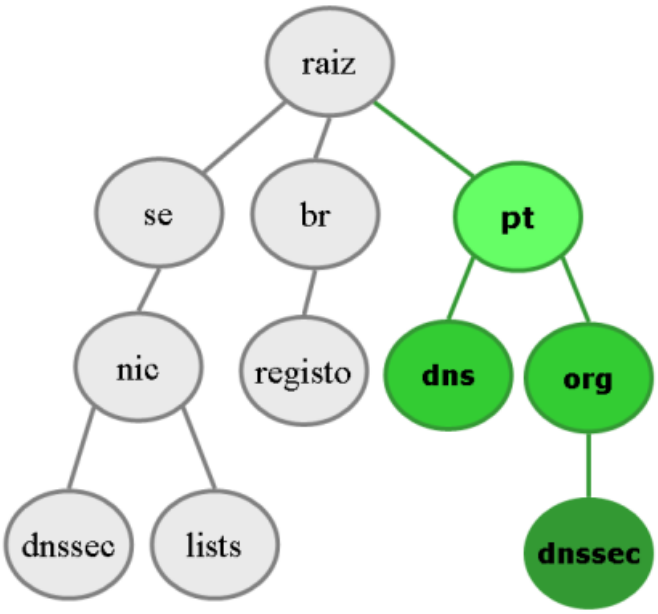

Figura 2.1: Estrutura em árvore do DNS

A tarefa de atribuir nomes a servidores e domínios de rede é conseguida criando um relação hierárquica entre os domínios, com os servidores como últimos descendentes da cadeia e uma raiz ("root") artificial como topo desta.

Adicionando etiquetas de nomes umas a seguir às outras criando um caminho do servidor até à raiz, numa forma de árvore hierárquica, um identificador único, memorizável e de fácil utilização é criado e designa-se de nome de domínio.

O DNS providencia resolução em ambas as direcções, isto é, dado um domínio, devolve o endereço IP apropriado e vice versa, através da utilização dos resource

records. Estes RRs fazem parte da configuração dos domínios e encontram-se armazenados em ficheiros de zona que contém os dados necessários para resolver os pedidos de nomes associados ao domínio da qual a zona é responsável. A Tabela 2.1 lista alguns dos principais tipos de RRs que se podem encontrar nos ficheiros de zona presentes nos servidores DNS:

SOA	Autoridade para os dados do domínio
NS	Servidor de nomes para o domínio
A	Endereço IP (Internet Protocol)
PTR	DNS Reverso, de endereços IP para nomes
CNAME	Nome canónico (Alias)
TXT	Informações textuais
WKS	Well-Known Services
HINFO	Informação do servidor (Host Information)
MX	Mail Exchanger

Tabela 2.1: Tipos de resource records (RRs)

O espaço de nomes de domínio é uma especificação de uma árvore estruturada (ver Figura 2.2). A raiz da árvore trata-se da raiz do domínio seguida pelos seus filhos, os domínios de topo (TLD), que podem conter diversos níveis de subdomínios até um total de 127, e o nome completo de domínio não pode ultrapassar os 255 caracteres.

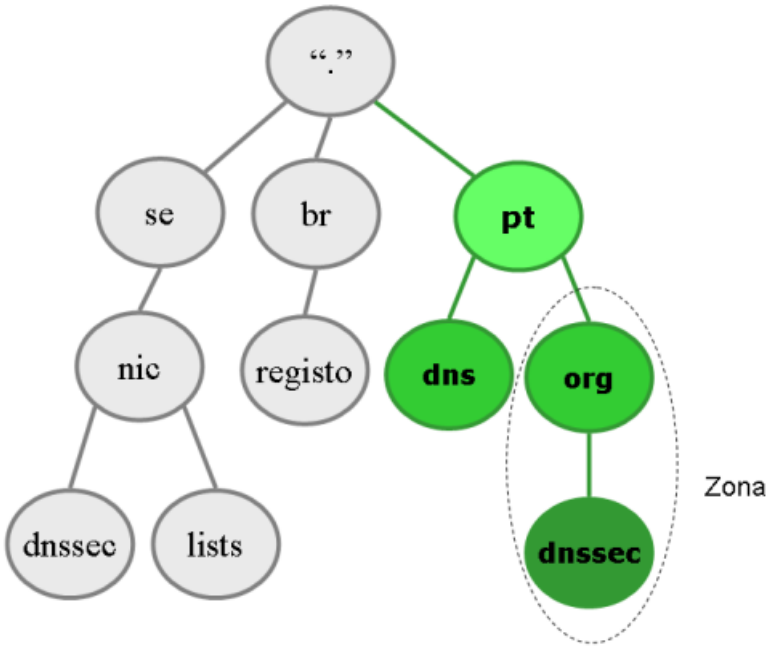

Figura 2.2: Zona de domínios

Os nomes de domínios consistem na concatenação das etiquetas de cada nó (domínios) separadas por ponto, no caminho que vai desde a folha, que representa a máquina actual, até à raiz. Os domínios são sub-árvores do espaço de nomes.

No exemplo da Figura 2.2, *"dnssec.org.pt"* é o nome de domínio de um nó cujo nome é *'dnssec'*, o seu pai é *'org'*, o seu avô é *'pt'* e o seu bisavô a raiz.

Uma zona é um conjunto de domínios, subdomínios e máquinas, a quem foi delegada autoridade de gestão pelo nível hierarquicamente superior e também inclui todos os nomes de domínio de níveis inferiores que ainda não tenham sido delegados.

Na Figura 2.3 é exemplificada uma delegação de um subdomínio onde são indicados os RRs do servidor de nomes (NS) e o respectivo endereço IP.

```
;
;  Delegação do subdomínio:  dnssec.org.pt.
;
dnssec                                  NS      ns.dnssec.org.pt.
ns.dnssec.org.pt.                       A       193.136.7.1
;  Fim da delegação
```

Figura 2.3: Delegação de um subdomínio

É superior hierárquico de todas as zonas, o nível máximo dos domínios de topo, este denomina-se de raiz e é representa-se simbolicamente com um ponto.

Uma zona pode ter vários servidores de DNS e cada servidor de DNS servir mais do que uma zona. No entanto, um mesmo servidor DNS não pode servir duas zonas hierarquicamente relacionadas. Isto é, não pode ser servidor DNS da zona A e B simultaneamente, se a zona A delegou autoridade na zona B, ou se a zona B delegou autoridade na zona A.

2.1.2 Vulnerabilidades de segurança

É do conhecimento geral que o serviço de nomes DNS, consistindo num protocolo de comunicação de elevada importância para o funcionamento de infra-estruturas globais como a Internet, apresenta inúmeras fragilidades.

A resolução de nomes é um dos aspectos mais críticos de interacção entre pessoas, serviços e máquinas. No universo da Internet existem inúmeros servidores de nomes, com graus de abrangência muito distintos, que estão permanentemente envolvidos quando se trata de estabelecer uma interacção entre duas entidades, sejam elas pessoas, serviços ou máquinas.

A interferência com o serviço DNS permite realizar ataques de personificação de máquinas ou serviços. A personificação de serviços, ou máquinas onde os mesmos se executam, consiste em enganar os seus clientes e levá-los a comunicar com um servi-

dor impostor. Para isso há que conduzir a comunicação do cliente para o servidor impostor sem que o cliente e o servidor legítimo se apercebam.

Uma forma de efectuar personificações de servidores é registando nomes DNS fraudulentos, aparentando representar uma entidade que efectivamente, não representam. É relativamente fácil enganar utilizadores fornecendo-lhes nomes DNS credíveis mas enganadores.

Uma outra forma de promover o uso de servidores falsos é interferir com o processo de resolução de nomes DNS. Este processo é conhecido como DNS spoofing.

A especificação inicial do DNS não contemplava quaisquer políticas ou mecanismo de segurança para evitar ataques à resolução de nomes. Pelo contrário, o seu desenho contemplou fundamentalmente aspectos de eficácia, eficiência e escalabilidade. Por este facto, essa especificação possuía diversas vulnerabilidades de segurança que foram exploradas aos longo dos anos para induzir erros na resolução de nomes DNS. Como reacção, apareceram diversas políticas e mecanismos que procuram eliminar e minizar esses riscos, como é o caso das extensão de segurança DNSSEC [5].

A técnica mais frequente para efectuar DNS spoofing passa pelo envenenamento de caches DNS (DNS cache poisoning). O princípio é simples: quando um servidor DNS pede a outro que lhe resolva um nome a resposta é autenticada de forma fraca. Qualquer um pode enviar respostas falsas para um servidor DNS e, se as mesmas forem aceites, introduzir resoluções de nomes erradas. Como os servidores DNS, por razões de eficiência, vão guardar essa informação em cache (memória temporária) durante algum tempo, tempo esse que depende do servidor e da informação afecta ao nome, enquanto a informação errada estiver em cache esta última está "envenenada" e permite efectuar DNS spoofing.

O envenenamento da memória de cache pode ser aplicado maliciosamente para fins como:

- Indisponibilidade do serviço (DoS - Denial of Service);
- Personificação de entidades de confiança;

Transferência de zona

Pelo papel importante que as zonas desempenham no DNS, pretende-se que estas estejam disponíveis aos clientes DNS a partir de mais de que um servidor de DNS na rede para fornecer disponibilidade e tolerância a falhas aquando da resolução de consultas de nomes. Caso contrário, se for utilizado um servidor único e este não estiver a responder, as consultas de nomes na zona poderão falhar.

Para os servidores adicionais hospedarem uma zona, é necessário que as transferências de zona efectuem a replicação e sincronizem todas as cópias da zona utilizada em cada servidor configurado para hospedar a zona.

Quando é adicionado um novo servidor de DNS à rede e é configurado como um servidor secundário para uma zona existente, este efectua uma transferência inicial total da zona para obter e replicar uma cópia completa dos resource records da zona. Mas por vezes ocorrem ataques que visam a obtenção da zona por meio de transferência da mesma para futuras modificações ou exposição da informação para interpretação da arquitectura do sistema. Deve-se, portanto, limitar os sistemas que podem fazer a transferência de zona dos seus servidores de nomes.

Envenenamento da memória temporária DNS

Seguindo o exemplo que se apresenta, vejamos como é que uma técnica de DNS spoofing pode funcionar:

Um utilizador quer ligar-se a um servidor remoto 'A' com um cliente telnet. A aplicação do cliente telnet questiona o cliente DNS (Resolver) para determinar o endereço IP do servidor 'A'. O cliente recebe uma resposta falsa do servidor DNS que o encaminha para um servidor remoto gerido pelo atacante (que alterou previamente na memória cache do servidor DNS um endereço IP incorrecto). Por causa dos dados manipulados, a aplicação telnet inicia uma sessão TCP com o servidor errado 'B'. O utilizador não se apercebe e envia o seu login e password directamente para o atacante. O atacante atinge assim o seu objectivo e restaura a ligação. O utilizador recebe uma mensagem de erro e repete a sua tentativa de login, desta vez com sucesso, porque desta vez o cliente DNS obteve o endereço de IP correcto da resposta ao servidor 'A' que não se encontra manipulado.

O cenário demonstrado torna claro que quando um atacante corrompe um servidor DNS com informação maliciosa pode redireccionar tráfego sempre que quiser, para onde quiser. Isto é possível porque quase todas as aplicações dependem da resolução de nomes para endereços providenciada pelo DNS. As técnicas de redireccionamento do tráfego da rede por manipulação da informação do DNS são conhecidas como "DNS hijacking", "DNS spoofing" ou "DNS poisoning".

Ao longo dos anos os atacantes registaram os seus próprios servidores de DNS e manipularam servidores DNS bem conhecidos. Um servidor DNS manipulado que está a responder a mensagens poderá incluir dados na secção adicional, que não estão directamente relacionados com a resposta. O servidor de DNS não desempenha nenhuma verificação para assegurar que esta secção adicional está correcta ou até relacionada de algum modo com a resposta.

Tipos de Ataques DNS

O serviço DNS tem um determinado conjunto de vulnerabilidades, existindo alguns principais pontos de ataque, tais como:

- "Cache Spoofing" - Corrupção da informação em cache consiste na introdução de dados com falsa informação na memória de cache, de modo a possibilitar que um atacante redireccione um determinado domínio para um servidor próprio, recebendo assim todas as informações que os utilizadores enviarem, inclusivamente senhas de acesso.
- "Traffic diversion" - Dispersão de tráfego é um ataque que gera o consumo de largura de banda e sobrecarga na rede e dos recursos do sistema;
- "Distribuited denial-of-service (DDoS)" - Ataque distribuído de negação de serviço nos servidores de nomes;
- "Buffer Overruns" - Consultas recursivas a um domínio causando overflow do buffer provocando a paragem do sistema ou produção incorrecta de resultados;

Estes problemas de segurança necessitam de solução de modo a assegurar um serviço mais confiado e fidedigno. A Figura 2.4 representa um fluxo de transmissão de dados DNS e ilustra como é que alguns dos ataques às vulnerabilidades mais conhecidas do DNS actuam nos diversos componentes do sistema.

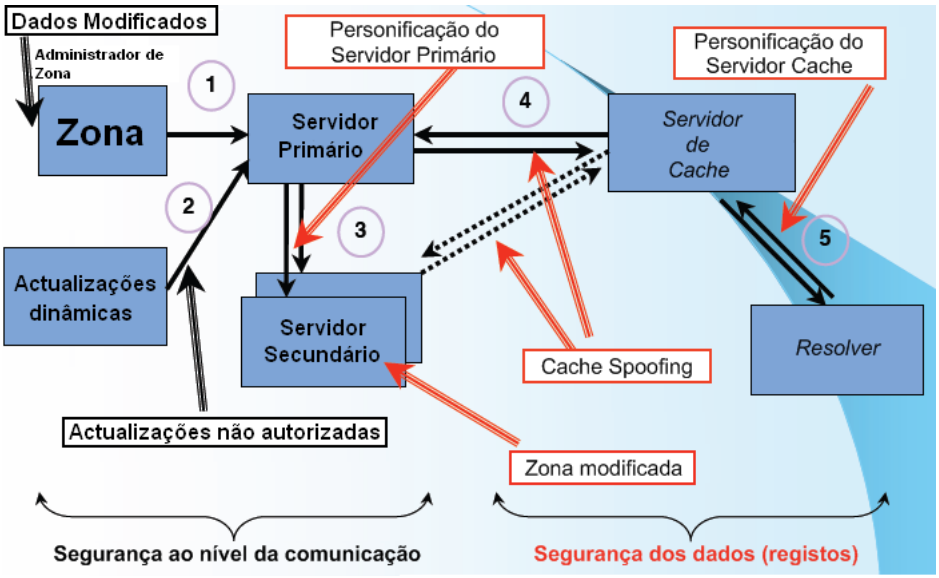

Figura 2.4: Vulnerabilidades do serviço DNS

O DNSSEC previne um tipo de ataque específico, o envenenamento de cache do DNS, para tal, permite que os servidores de DNS consigam autenticar as respostas das resoluções de nomes. Se um atacante conseguir falsificar um endereço IP de um determinado site, o servidor DNS usando o DNSSEC, poderá verificar que a resposta não é a correcta e saberá que deve descartá-la e tentar descobrir o novamente o endereço real do site até obter uma resposta válida.

2.1.3 Origem do DNSSEC

Em resposta às vulnerabilidades de segurança do DNS, o IETF (Internet Engineering Task Force) formou um grupo de trabalho para adicionar extensões da segurança (DNSSEC) ao protocolo existente [6].

Estas extensões ao protocolo original consistem numa hierarquia de assinaturas criptográficas que providenciam autenticação da origem dos dados e integridade nas mensagens DNS e autenticação da resposta da não existência de um domínio. Estas medidas protegem contra memórias cache e transmissões modificadas contribuindo para a segurança do utilizador final, e por consequência aumenta a confiança deste no uso da Internet e nos sistemas (detalhes na secção 3.1.2).

A fim de ganhar aceitação, o grupo de trabalho reconheceu que o DNSSEC deve fornecer compatibilidade e deve ter a possibilidade de coexistir com implementações de DNS não seguras. Isto permite que os domínios migrem para DNSSEC quando estiverem preparados e permite menos complexidade quando forem efectuadas actualizações. Significa também que o software do lado do cliente, que não tenha suporte ao DNSSEC, consiga também processar correctamente os dados recebidos de um servidor de nomes com DNSSEC.

Apesar de estar em desenvolvimento há mais de 10 anos, o DNSSEC ainda não está a ser implementado na grande maioria das organizações. Quanto maior a Internet se torna, maior é a complexidade que a implementação do DNSSEC tem e este problema incluiu questões como desempenho, gestão de chaves e aspectos organizacionais.

As razões do atraso de uma implementação de DNSSEC em clientes de DNS reside na necessidade de bibliotecas de programação que providenciem os mecanismos definidos nos novos RFCs (Request for Comments). Infelizmente a biblioteca LWRL (Lightweight Resolver Library), que vem com a distribuição do BIND (Berkeley Internet Name Domain) versão 9, não é suficiente para estes requisitos.

O BIND, tendo sido inicialmente designado como Berkeley Internet Name Daemon, é uma ferramenta para o protocolo DNS das mais utilizado na Internet, especialmente em sistemas do tipo Unix, sendo considerado, praticamente, como uma ferramenta padrão. Foi criado por quatro estudantes da Universidade de Berkeley

com o objectivo de garantir competitividade com as ofertas de servidores DNS da Microsoft e actualmente é suportado e mantido pelo Internet Systems Consortium.

Para a versão 9, o BIND foi praticamente redefinido, passando a suportar, entre outras funcionalidades, a extensão DNSSEC e os protocolos TSIG [7] e IPv6. As extensões de segurança DNSSEC foram financiadas por militares que perceberam a importância da segurança nos servidores DNS. No entanto, as especificações de Olaf Kolkman's para DNSSEC na linguagem Perl [8] são as únicas a cumprir correctamente as especificações do RFC.

A versão corrente do DNSSEC foi publicada em Março de 2005 e está disponível nestes 3 documentos: RFC4033 [9], RFC4034 [10] e RFC4035 [11].

2.1.4 Trabalho Relacionado

Projectos piloto de concretização do DNSSEC foram bem cedo submetidos pela Holanda e pela Suécia. A Suécia foi o primeiro TLD (Top-level domain) a assinar a sua zona. Os projectos iniciais resultaram em experiências práticas de desenvolvimento, preparação de material de treino e uma maior compreensão de algumas das limitações da especificação e esclarecimento de questões em aberto.

Esta experiência tem sido expandida pela recente publicação do Sweden's National Post and Telecom Agency, Post-och Telestyrelsen, dos seus testes de implementação e administração do DNSSEC num subdomínio do domínio .SE.

A Tabela 2.2 apresenta alguns projectos já desenvolvidos:

Nome	URL
DNSSEC(.se)	http://dnssec.nic.se/
Infrastructure DNSsec et Applications	http://www.idsa.prd.fr/index.php
NeuStar Pilot in .US (concluded)	http://www.potaroo.net/iepg/november 2004/DNSSECtrial-in-us.pdf
NIST Advanced Network Technologies Division, Internet Infrastructure Protection, Domain Name Security Project	http://www.antd.nist.gov/iipp.shtml http://www-x.antd.nist.gov/dnssec
NLnetLabs DNSSEC HOWTO	https://www.ripe.net/projects/disi
Root Server Testbed Network	http://www.rs.net/
Internet2 Cross-Signing Pilot	http://www.dnssec-deployment.org/internet2/
DNS Security (DNSSEC) Testbed	http://www.pir.org/RegistrarResources/ DNSSecurityTestbed.aspx
registro.br DNSSEC	http://registro.br/info/dnssec.html

Tabela 2.2: Projectos desenvolvidos e base de dados de teste

Alguns dos desenvolvimentos principais desde o lançamento dos RFCs em Março de 2005 incluem o seguinte:

- .SE, o Registry nacional da Suécia [12] que foi o primeiro ccTLD a implementar DNSSEC na sua zona, lançou o serviço comercial de DNSSEC [13];
- RIPE NCC, o fornecedor de serviços da infraestrutura da Internet Europeia, implementou o DNSSEC na árvore reversa;
- O segundo ccTLD a disponibilizar o serviço de DNSSEC na sua zona foi o Registry de Puerto Rico (.PR) com toda a zona assinada;
- O Registry da Bulgária (.BG) tem mais de 30 delegações de zonas assinadas e seguras;
- NIC México e Tecnológico de Monterrey Campus Monterrey patrocinaram o DNSSEC México experimental para permitir aos seus membros experimentar e tornar-se familiares com a tecnologia e para analisar as introduções operacionais e técnicas de uma distribuição do futuro DNSSEC em .MX;
- Internet2, um consórcio das principais universidades dos E.U., laboratórios de pesquisa e parceiros internacionais, iniciaram um projecto piloto e organizaram um grupo de trabalho que se encontra mensalmente por meio de video-conferência e nos workshops e conferências dos membros Internet2;
- .ORG manteve um testbed para permitir aos seus registrars testarem sistemas com suporte a DNSSEC;
- .AERO expressou o interesse em desenvolver o DNSSEC embora planos firmes ainda não tenham sido anunciados;
- A Microsoft anunciou planos para fornecer suporte DNSSEC nos seus servidores DNS no service pack 1 do Longhorn, espera-se que fique disponível em 2008;
- O National Institute of Standards and Technology dos Estados Unidos (NIST), um dos parceiros da iniciativa de coordenação do desenvolvimento, realizou o lançamento de uma Publicação Especial 800-53, revisão 1, Controlos Recomendados da Segurança para Sistemas de Informação Federal em Dezembro de 2006. O guia inclui um plano para uma distribuição inicial da tecnologia DNSSEC dentro dos sistemas informáticos federais e especifica controlos mínimos da segurança necessários para complementar os Padrões Federais de Processamento de Informação (FIPS) requeridos pela Informação Federal de Gestão da Segurança (FISMA). As agências federais dos Estados Unidos terão

um ano após a publicação final para ficarem em conformidade com os novos padrões. (Para mais informação, ver a implementação do projecto da FISMA, http://csrc.nist.gov/sec-cert/);

- O domínio de topo do Brasil .br [14] já é uma zona assinada com DNSSEC desde o início do mês de Junho, tratando-se do terceiro ccTLD operacional com extensões de segurança ao DNS. O técnico responsável Frederico Neves reporta que o ccTLD .br, assim como 4 das suas hierarquias (zonas filhas), foram assinadas a 4 de Junho e espera-se que zonas adicionais venham a ser assinadas num futuro próximo. A chave pública (KSK) encontrar-se em https://registro.br/ksk/, e a publicação de chaves DNSSEC de .br e as políticas de gestão estão disponíveis em http://registro.br/info/dnssec-policy-en.html.

2.2 Definição dos Objectivos

Uma vez apresentado o âmbito do projecto, torna-se agora necessário definir qual o seu foco e o que se pretende atingir.

As vulnerabilidades de segurança do protocolo DNS base e os recentes desenvolvimentos nesta área por parte de outras entidades gestoras de domínios de topo movem-nos no sentido de preparar de imediato todos os procedimentos necessários para fornecer este novo serviço aos detentores de domínios .PT. No entanto, o DNSSEC ainda tem algumas questões por resolver e a sua adopção tem implicações a ter em conta para a garantia de um bom funcionamento do serviço e da rede nas organizações.

Com este trabalho pretende-se fazer uma análise detalhada dos efeitos da implementação do DNSSEC no serviço prestado pela entidade gestora do domínio de topo .PT [3] bem como da necessidade de adopção de novos processos de trabalho.

Este projecto será a base de preparação para a possível entrada em produção do novo serviço bem como a base de decisão em se avançar nesse sentido.

2.3 Planeamento

Esta secção explica como foi projectado, organizado e escalonado o trabalho. Vários factores foram tidos em conta na definição do projecto e o modo como este seria concretizado. Estes aspectos são fundamentais no desenvolvimento de um projecto e assentam nos fundamentos de engenharia de software.

2.3.1 Metodologia utilizada

Depois do estágio ter sido atribuído seguiu-se um período de levantamento de informação e análise de soluções existentes para o problema da segurança do protocolo DNS e viabilidade da implementação das extensões de segurança (DNSSEC).

O estudo comparativo das várias implementações já existentes permitiu uma maior consciencialização do desenvolvimento deste protocolo, o que desencadeou todo o processo de análise técnica e definição de requisitos funcionais e técnicos necessários à instalação piloto de DNSSEC no sistema de registo de domínios de .PT.

Tratando-se de uma instalação piloto e em processo de estudo comportamental não foi contactada nenhuma entidade externa para a adesão a este serviço, mas foram criados internamente domínios de teste com os quais se procedeu de forma a entender todos os requisitos necessários a ter em conta no lançamento oficial deste novo serviço.

Como já foi referido, a implementação do serviço foi desenvolvida internamente na FCCN e implicou um processo cuidado e moroso para que a instalação piloto não interferisse de modo algum com a gestão diária do funcionamento do DNS e que não provocasse a quebra do serviço de registo de domínios.

2.3.2 Calendarização

Inicialmente foram definidas tarefas e prazos a cumprir no planeamento do projecto mas cedo se percebeu que o planeamento original teria que ser redefinido com tarefas mais adequadas ao tempo disponível e à complexidade do projecto. As tarefas realizadas, não previstas inicialmente, foram as seguintes:

- Houve uma redifinição das tarefas de configuração passando da zona .pt para a hierarquia org.pt;
- Migração dos serviços de um servidor DNS para uma nova máquina;
- Disponibilização da zona .pt em forma hierárquica em relação à zona de org.pt
- Criação de “scripts” automatizadas para assinaturas de domínios massificadas;
- Actualização das versões de instalação da ferramenta BIND (Berkeley Internet Name Domain) para versão 9.3.1 ou superior em algumas máquinas de modo a fornecerem suporte a DNSSEC;
- Realização de um Workshop no âmbito do projecto desenvolvido

Apesar das várias redefinições de tarefas o planeamento em termos de calendarização não sofreu desvio significativo tendo este projecto sido concluído próximo da data inicialmente prevista (planeamento rectificado e o respectivo mapa de gantt são apresentados no anexo A).

Capítulo 3

Trabalho Realizado

Este capítulo descreve o trabalho realizado ao longo do projecto, apresentando as ferramentas utilizadas e desenvolvimentos efectuados, assim como a análise dos resultados obtidos.

3.1 Análise Funcional

Como já foi referido anteriormente, as extensões de segurança ao protocolo DNS original vêm implementar uma hierarquia de assinaturas criptográficas que permitem garantir que os dados recebidos provieram de facto da origem esperada (autenticação da origem dos dados), que os dados não foram alterados por outrem durante a transmissão (integridade dos dados) e a não existência de um nome ou tipo.

Antes de se entrar em mais detalhes nestas características de segurança é necessário rever um conceito sempre associado à autenticidade de informação que é a utilização de criptografia de chave pública.

3.1.1 Criptografia e Assinaturas

A criptografia é uma ciência que permite escrever de forma a ocultar conteúdos. O objectivo da criptografia é permitir que um conjunto limitado de entidades, tipicamente duas, possam trocar informação que é ininteligível para terceiros ou que seja possível guardar e transmitir informação privada em redes abertas (como a Internet) sem o perigo de ser lida ou modificada por alguém que não seja o destinatário final da mensagem.

A criptografia baseia-se no uso de cifras. Uma cifra é uma técnica concreta de criptografia, isto é, uma forma específica de ocultar informação. Assim, uma cifra transforma um texto em claro num texto cifrado ou criptograma. A operação

inversa é a decifra, que transforma um criptograma no texto em claro original como ilustra a Figura 3.1. Se a decifra for mal efectuada, ou porque o criptograma está corrompido ou porque houve uma má escolha de algoritmos ou chaves de decifra, então o resultado é imprevisível.

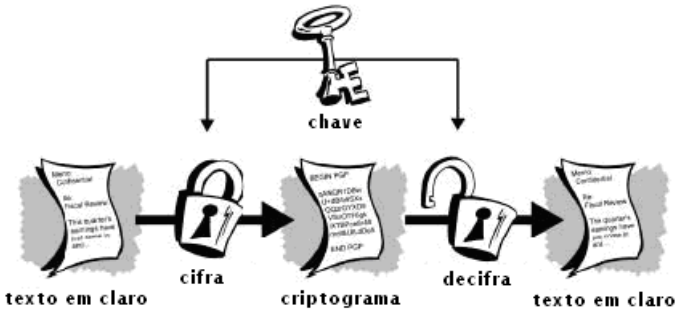

Figura 3.1: Criptografia

A operação da maioria das cifras e decifras é definida através da especificação de um algoritmo e de uma chave. O algoritmo define o modelo de transformação de dados, a chave é um parâmetro do algoritmo que permite variar o seu comportamento de forma complexa.

Criptografia assimétrica

A criptografia assimétrica, ou de chave pública, utiliza um par de chaves distintas mas relacionadas: uma chave pública para cifrar e uma chave privada para decifrar, e não é possível, dada a chave pública, calcular a correspondente chave privada (ver Figura 3.2).

As cifras permitem ainda efectuar a cifra ao contrário, cifrando com a chave privada e decifrando com a pública, o que não tem grande interesse para esconder a informação, mas é importante para garantir a sua autoria.

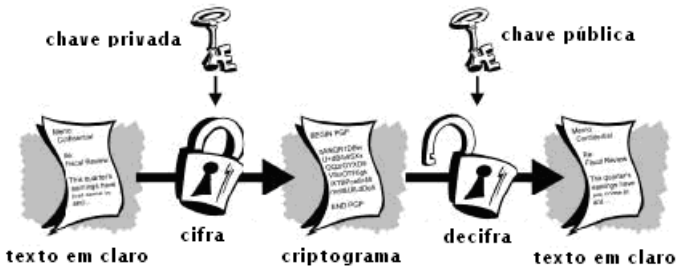

Figura 3.2: Criptografia Assimétrica

Os pares de chaves assimétricas são personalizados, ou seja, são associados a pessoas, serviços ou servidores. A componente privada deve ser mantida em segredo,

devendo ser apenas do conhecimento e da utilização da entidade a que se encontra associada. A chave pública pode (e deve) ser ampla e publicamente divulgada para poder ser utilizada por qualquer entidade.

Em termos operacionais as cifras assimétricas têm como principal vantagem o facto de exigirem menos chaves para efectuar interacções seguras porque permite uma relação de muitos para um.

Em termos administrativos os principais problemas subjacentes à utilização de criptografia assimétrica são:

- Confinamento rigoroso das chaves privadas aos legítimos detentores;
- Distribuição fidedigna de chaves públicas a todos os que as pretendem usar;
- Gestão do tempo de vida dos pares de chaves;

Assinaturas digitais

Um dos maiores benefícios da criptografia de chave pública é a possibilidade do uso de assinaturas digitais. As assinaturas digitais permitem ao destinatário de uma mensagem verificar a autenticidade da origem da informação, e verificar também se a informação não foi alterada durante o trajecto. Logo, assinaturas digitais de chave pública fornecem autenticação e integridade de dados.

Como mencionado, o objectivo das assinaturas digitais é ir mais longe na garantia de origem e assegurar a autoria de uma mensagem perante terceiros. Uma mensagem assinada digitalmente fica associada a uma e uma só entidade e a assinatura deverá poder ser validada universalmente. A criptografia assimétrica é a que melhor se adequa a este fim, uma vez que os pares de chaves têm um cariz pessoal, isto é, cada par de chaves pertence apenas a uma entidade.

Tecnicamente, e de uma forma simplificada, uma assinatura digital de um documento consiste na cifra do mesmo com a chave privada do autor e não serve para esconder o documento original mas sim para garantir, a quem a decifrar com a chave pública correspondente, que o documento não foi modificado.

Devido ao elevado custo computacional das cifras assimétricas, não interessa cifrar a totalidade do documento a assinar mas sim um valor de pequena dimensão que represente o mesmo, ou seja, uma síntese (hash) do mesmo. Usando a síntese, obtém-se uma maior eficiência na geração e validação de assinaturas digitais e obtêm-se assinaturas mais reduzidas.

Se, na validação da assinatura, não for possível verificar a equivalência, significa que ou o texto e a informação adicional foram alterados ou a assinatura foi alterada.

A Figura 3.3 ilustra o processo de criação de uma assinatura digital associada a um determinado documento.

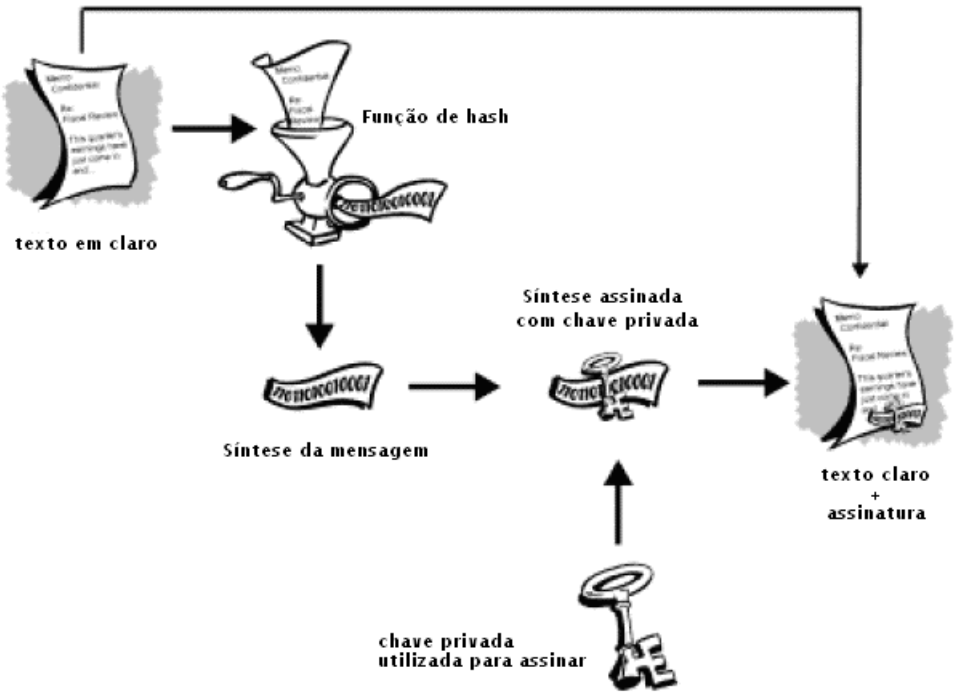

Figura 3.3: Assinatura Digital

3.1.2 Extensões ao protocolo DNS

Estas extensões ao protocolo original consistem numa hierarquia de assinaturas criptográficas que providenciam autenticação da origem dos dados do DNS, integridade e autenticação da resposta da não existência de um domínio. Estas medidas protegem contra corrupção de memórias de cache e transmissões modificadas e contribuem para o aumento da confiança na Internet e nos sistemas.

O DNSSEC não garante a confidencialidade dos dados nem protege contra ataques de negação do serviço (DoS).

Cada domínio, quer seja único ou seja um TLD, pode ter um conjunto de resource records (RRs) a ele associado. Para um domínio isolado, o resource record mais comum é o do tipo A (address) que faz corresponder a um domínio o respectivo endereço IP, mas existem muitos outros. Quando um cliente de DNS pergunta por um domínio a um servidor de DNS, o que recebe de volta são os resource records associados a esse domínio.

A função real do DNS é fazer corresponder nomes de domínios aos seus respectivos resource records. Estes são divididos em classes e tipos e actualmente existe uma grande variedade de tipos. Ao conjunto de resource records com o mesmo nome de domínio, classe e tipo é denominado "Resource Record Set"(RRset).

Alguns tipos mais comuns de resource records são:

- SOA - Indica onde está delegada a autoridade da zona
- NS - Indica um servidor de nomes para a zona
- A - Atribuiu o nome a um endereço

O DNSSEC introduz resource records adicionais que se dividem em quatro tipos diferentes. São eles: DNSKEY, RRSIG, NSEC e DS.

DNSKEY

Todas as zonas DNS assinadas têm associado um par de chaves privada e pública. A chave privada mantém-se (muito bem guardada) em segredo com o administrador da zona. A chave pública associada à zona é publicada num ficheiro e designa-se DNSKEY.

O DNSKEY é o resource record que contém as chaves públicas (resultantes de um algoritmo de encriptação assimétrico) para suporte do DNSSEC, chaves estas que permitem verificar as assinaturas dos RRs de uma zona previamente assinados recorrendo à chave privada correspondente.

A Figura 3.4 [15] é um exemplo deste tipo de RR e identifica os vários componentes.

Figura 3.4: Exemplo de um DNSKEY resource record

As chaves públicas utilizadas em operações de assinatura de zonas podem ser de dois tipos. Temos a chave pública ZSK (Zone Signing Key) que é utilizada para assinar os resource records numa zona e a chave pública KSK (Key Signing Key) que por sua vez é utilizada para assinar as ZSKs, reforçando o processo de encriptação.

O DNSKEY pode ser criado a partir do utilitário *dnssec-keygen* fornecido na ferramenta de software BIND.

RRSIG

Como foi já mencionado, um RRset é um conjunto de resource records de uma zona DNS que partilham em comum um nome, uma classe e um tipo e por esse motivo estes são agrupados.

O RRSIG, representado na Figura 3.5 [15], consiste no RR que contém a assinatura digital de um RRset específico com uma determinada chave (DNSKEY).

Figura 3.5: Exemplo de um RRSIG resource record

Cada RRset numa zona assinada terá um resource record RRSIG contento a síntese do RRset criado utilizando o resource record DNSKEY de ZSK (Zone Signing Key). O RRSIG é único, possui uma validade inicial (inception) e final (expiration) e pode ser gerado automaticamento através do utilitário *dnssec-singzone* fornecido com o BIND versão 9 ou superior.

NSEC

O NSEC, que deriva da nomenclatura "Next Secure", é o resource record que vem permitir autenticar a resposta da inexistência de um domínio, ou seja, que o nome de domínio pedido na realidade não existe.

Este RR disponibiliza duas informações distintas, a do próximo nome seguro (numa ordenação canónica da zona) e os tipos de RRsets existentes para um nome.

O conjunto completo de resource records NSEC de uma zona revelam quais os que RRsets que efectivamente existem na zona e formam uma cadeia de nomes de domínios em que o último resource record da zona aponta para o primeiro (SOA) permitindo fechar a cadeia criando um ciclo.

A revelação desta informação é utilizada para providenciar autenticidade aquando a inexistência de uma resposta, isto é, se o nome ou tipo consultados realmente não existem e a situação encontrada não se trata de um ataque ao DNS e por consequente o acesso a determinado serviço não foi permitido (DoS).

A Figura 3.6 [15] exemplifica um resource record NSEC onde se pode verificar que o nome pc2.xpto.pt não existe, pois estando a zona ordenada canonicamente, o nome que vem depois de pc1.xpto.pt é o pc3.xpto.pt, logo não existe nenhum nome válido entre os mencionados. Pode-se também concluir que para o nome pc1.xpto.pt não existe associado nenhum resource records do tipo MX (Mail eXchanger), por isso se for realizado um pedido de RR MX deste domínio a resposta terá que ser obrigatoriamente negativa.

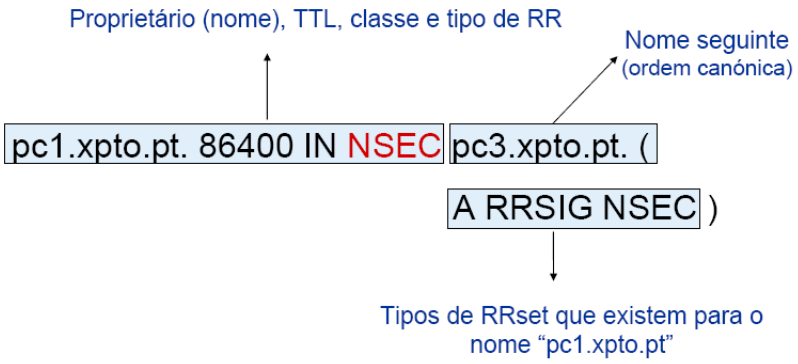

Figura 3.6: Exemplo de um NSEC resource record

DS

A questão da validação da chave pública da zona ainda continua por resolver após a apresentação dos três primeiros tipos de resource records. Um atacante só necessita de fornecer um DNSKEY e os dados RRSIG que correspondam aos dados do RRset fictício de modo fazer com que a resposta pareça "autêntica".

A aproximação adoptada pelo DNSSEC é a de utilizar uma cadeia de confiança dentro da delegação hierárquica da estrutura do próprio DNS. À excepção da zona "." (root), todas as zonas DNS têm uma zona pai. O resource record DS (Delegation Signer) contém uma síntese (hash) da chave pública das zonas dos filhos. Este resource record é assinado pela chave privada da zona pai ficando com o resource record RRSIG correspondente.

Consistindo o DS na síntese referente a um resource record DNSKEY, este serve para informar que existe uma cadeia de confiança entre um domínio e os seus sub-domínios e indica que a zona delegada é assinada e qual a chave pública utilizada nessa zona.

Como o resource record DS é assinado pela zona pai, esta zona tem a autoridade sobre o respectivo resource record não devendo este aparecer nas zonas filhas e funcionará como um ponteiro para a cadeia de confiança (chain trust). A cadeia de confiança garante a autenticidade das delegações de uma zona até um ponto de confiança, ponto esse que se pode tratar de uma chave ancorada ou a utilização de DLV (DNSSEC Lookaside Validation [16]), isto é, pontos de confiança ancorados fora da cadeia de delegação DNS.

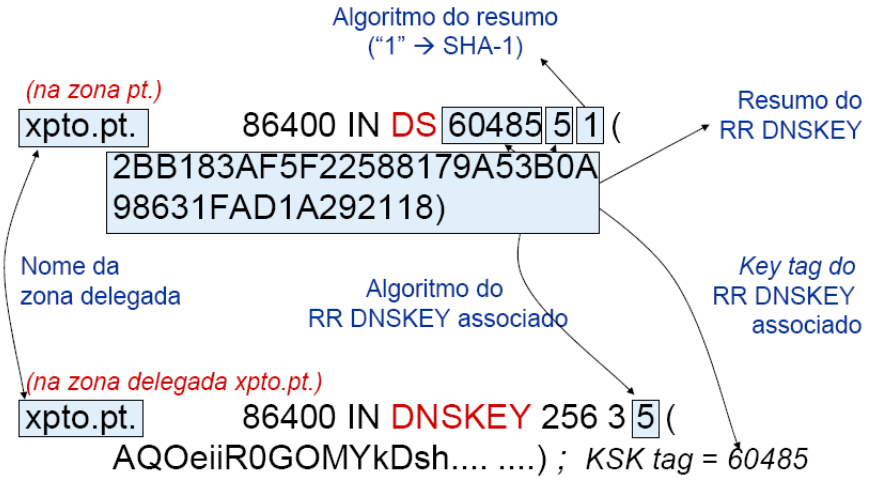

Figura 3.7: Exemplo de um DS resource record

Como ilustrado na Figura 3.7 [15] um RR DS armazena a informação necessária para a realização do processo de autenticação do DNSKEY, tais como, a etiqueta

(tag) da chave pública (KSK) do servidor filho, uma síntese (resumo) do respectivo resource record DNSKEY cifrado com ZSK do servidor pai e o algoritmo utilizado na criação desse resumo.

Para validar a delegação de uma zona, o servidor pai utiliza o resource record DS, e este RR por sua vez valida a KSK (chave pública) do servidor filho.

A chave de confiança ideal seria o DNSKEY na zona root, mas na ausência deste ponto de confiança cada cliente DNSSEC tem de configurar o seu próprio sistema de validação com pontos de confiança conhecidos, fora da validação hierárquica, como por exemplo, através de uma autoridade certificadora.

Confidencialidade

O protocolo DNS foi desenvolvido com o intuito de tornar públicos os resource records dos domínios independentemente de quem lhes está a aceder. As extensões de segurança seguem essa mesma orientação e não adicionam qualquer tipo de característica de confidencialidade ao protocolo base.

Transferências seguras de zona

Apesar de o DNSSEC permitir autenticação da origem e integridade dos dados para os RRsets, não o consegue fazer para zonas inteiras e, deste modo, devem ser utilizados outros mecanismos como o TSIG [7], SIG(0) [17] ou IPsec [18] para proteger essas operações de transferência.

3.1.3 Algoritmos e tipos de síntese de DNSSEC

As extensões de segurança do DNS foram desenhadas para serem independentes dos algoritmos criptográficos.

Os RRs DNSKEY, RRSIG e DS usam um número de algoritmo que identifica o algoritmo criptográfico utilizado nesse resource record. O RR DS define ainda um tipo de resumo que identifica o algoritmo utilizado na criação da síntese.

Os clientes e servidores DNS que tenham suporte a DNSSEC devem implementar todos os algoritmos obrigatórios.

Alguns dos algoritmos presentes na Tabela 3.1 são usados unicamente para assinatura de zona (DNSSEC), outros apenas para mecanismos de transacção segura (SIG(0) e TSIG), e alguns em ambas as situações. Os que são usados na assinatura de zona podem aparecer em resource records DNSKEY, RRSIG e DS.

Os algoritmos e tipos de síntese definidos actualmente estão listados na Tabela 3.1 [10].

Value	Algorithm [Mnemonic]	Zone Signing	References	Status
0	reserved			
1	RSA/MD5 [RSAMD5]	no	[19]	not recommended
2	Diffie-Hellman [DH]	no	[20]	-
3	DSA/SHA-1 [DSA]	yes	[21]	optional
4	Elliptic Curve [ECC]			-
5	RSA/SHA-1 [RSASHA1]	yes	[22]	mandatory
252	Indirect [INDIRECT]	no		-
253	Private [PRIVATEDNS]	yes		optional
254	Private [PRIVATEOID]	yes		optional
255	reserved			
6 - 251	Available for assignment by IETF Standards Action.			

Tabela 3.1: Tipos de algoritmos

Tipos de síntese

O campo de tipo de síntese no resource record DS identifica o algoritmo criptográfico utilizado no cálculo da síntese aplicado à chave pública a que este resource record diz respeito.

A Tabela 3.2 [10] mostra os tipos de algoritmos actualmente definidos para esta operação.

Value	Algorithm	Status
0	Reserved	-
1	SHA-1	mandatory
2-255	Unassigned	-

Tabela 3.2: Tipos de síntese

Identificador da chave

O identificador da chave (key tag), presente nos resource records RRSIG e DS, permite seleccionar uma chave pública de forma eficiente. Na maioria dos casos, a combinação do nome de domínio, algoritmo e chave podem identificar univocamente um resource record DNSKEY. Ambos os resource records RRSIG e DS têm resource records DNSKEY correspondentes. Nestes RRs, o identificador da chave pode ser

usado para ajudar a seleccionar o resource record DNSKEY quando existe mais do que um resource record candidato disponível.

No entanto, é de salientar que este identificador não garante a unicidade de referência para um único resource record. É teoricamente possível dois resource records DNSKEY terem o mesmo nome de domínio, algoritmo e chave.

O identificador da chave é calculado através de um algoritmo simples de hash.

3.2 Adopção do DNSSEC

De modo a desenvolver o DNSSEC operacionalmente, os servidores com suporte a DNSSEC devem somente desempenhar a inclusão automática de resource records quando há uma indicação explícita que o *Resolver* (cliente DNS) pode compreender esses RRs.

3.2.1 Requisitos

Complexidade

Apesar de conter apenas algumas regras simples, o DNS tem-se desenvolvido num sistema enorme e complexo. O DNSSEC introduz complexidade adicional ao DNS, o que acarreta novas possibilidades de aparecimento de incoerências no código e de zonas mal configuradas. Em particular, a activação da verificação da assinatura de DNSSEC num cliente DNS pode fazer com que zonas legítimas se tornem inacessíveis devido a erros de configuração.

Alocação de maior largura de banda

A adopção do DNSSEC implica uma troca de mensagens de maiores dimensões. Em resposta a pedidos de dados em zonas assinadas, os servidores DNS com suporte a segurança vão responder com os resource records DNSKEY, RRSIG, NSEC e/ou DS. A adição destes novos RRs implica a alocação de uma maior largura de banda para se efectuarem as trocas de mensagens entre o servidor e o cliente. No entanto, a grande maioria dos pedidos efectuados inicialmente a zonas assinadas serão realizados por clientes sem suporte às extensões de segurança e esses resource records adicionais não trarão qualquer mais-valia para esses clientes.

Cientes deste facto, os membros do grupo de trabalho para o desenvolvimento do DNSSEC definiram desde logo uma sinalização a ser enviada por clientes e servidores de nomes recursivos de modo a informar os servidores de nomes autoritativos de que têm suporte a extensões de segurança e que pretendem receber todos os resource records necessários para verificação da assinatura da zona. Deste modo, evita-se uma sobrecarga desnecessária da rede.

Para além do exposto anteriormente, uma vez que o protocolo DNS utiliza datagramas UDP no seu modo de funcionamento padrão, e que esses datagramas estão limitados a 512 bytes, existe uma grande probabilidade em as respostas que incluem os novos resource records DNSSEC terem de ser truncadas. Nestes casos, o cliente reenvia o pedido utilizando TCP e isto resulta numa utilização significativamente maior da largura de banda da rede devido ao estabelecimento de ligações. O impacto destes pedidos TCP podem acarretar um grande aumento do tráfego da rede (em média, 5 pacotes por cada pedido/resposta em vez de apenas dois), um maior tempo de resposta devido aos tempos de ida-e-volta, um aumento de pedidos com falhas devido aos timeouts (limites de tempo de concretização) e um aumento significativo da carga de processamento dos servidores de nomes.

Para colmatar este aumento de carga na rede existe a necessidade de utilizar o mecanismo de extensão ao protocolo DNS designado por EDNS0 (Extension Mechanisms for DNS [23]). Este mecanismo permite o envio de mensagens de maiores dimensões, definindo uma sinalização no header (bit DO) que corresponde a "DNSSEC OK". Se o cliente enviar este bit a 1, significa que está preparado para receber os resource records de extensões de segurança para zonas assinadas. Caso contrário, o servidor de nomes irá responder apenas com os resource records do protocolo base.

3.2.2 Novas Vulnerabilidades

Varrimento da Zona

O DNSSEC garante a autenticidade da resposta da não existência de um nome ou tipo de resource record através de uma cadeia de nomes, na qual cada um indica o próximo nome existente na zona, formando uma sequência canónica. Os resources records que desempenham o papel desses apontadores são do tipo NSEC.

O motivo pelo o qual o DNSSEC adoptou a solução NSEC, é a necessidade de garantir que um nome não existe, o que corresponde a características de autenticidade.

No entanto, esta solução permite obter todo o conteúdo de uma zona com simples consultas de DNS, método conhecido por varrimento de zona (Zone Walking).

Deste modo o DNSSEC introduz a possibilidade de qualquer utilizador com boas ou más intenções obter todos os nomes de uma zona, por ordem canónica, ao percorrerem a cadeia de resources records NSEC. Embora por si só, não se trate de um ataque, a informação que é possível recolher por este método permite descobrir os servidores existentes numa rede, facilitando assim o acesso à arquitectura de rede e por consequência a possibilidade de um ataque.

A combinação de NSEC com informação fornecida pelo serviço Whois é potencialmente muito mais grave. O serviço Whois é um serviço público que fornece informações pessoais sobre os responsáveis de um dado domínio. Se um utilizador percorrer uma zona, obtendo a lista de nomes existentes nessa zona, e de seguida pesquisar os contactos associados, de cada um dos nomes no serviço Whois, irá obter uma grande quantidade de informação pessoal (endereços de mail, números de telefone, moradas, entre outros). Para fazer face ao problema de Zone Walking, foi criada a solução "DNSSEC Hashed Authenticated Denial of Existence" [24] mais vulgaremente conhecida por NSEC3.

Os resource records NSEC3 são assinados à semelhança dos resource records NSEC, mas em vez de incluir directamente o próximo nome (o que permitia percorrer a zona), o NSEC3 inclui o resultado cifrado de uma função de hash sobre o próximo nome. Inclui ainda uma componente adicional conhecida por sal (salt) que aumenta o grau de complexidade do acesso à informação, pois o campo sal é adicionado ao nome original do proprietário antes do hash ser realizado a fim de proteger contra ataques de dicionário. O NSEC3 é uma solução recente que ainda está em desenvolvimento, e a sua especificação actual ainda gera alguns conflitos com metodologias já existentes como as actualizações dinâmicas no DNS.

Ataque de processamento extra

As extensões do DNSSEC tornam o DNS vulnerável a uma nova classe de ataques de negação de serviço, baseada nas operações de criptografia processadas tanto pelos clientes como pelos servidores de DNS que suportam as extensões de segurança, uma vez que um atacante pode tentar consumir todos os recursos das suas vítimas através desse processamento.

Esta classe de ataques pode tomar pelo menos duas formas. Um atacante pode tentar consumir recursos de processamento extra de validação de assinaturas num cliente DNS com suporte a segurança alterando o RRSIG na resposta às mensagens ou através da construção desnecessária de cadeias de assinaturas. Um atacante pode também ser capaz de consumir recursos num servidor de nomes com suporte a segurança através do envio de mensagens de alteração dinâmica que forcem o servidor a re-assinar alguns RRsets na zona, de forma mais frequente do que o que

seria de esperar [25].

Com base numa análise de custo/benefício para a organização a usufuir da implementação do protocolo DNSSEC, medidas de precaução (como por exemplo, utilização de máquinas mais eficientes ou soluções de geração de assinaturas baseadas em hardware) podem ser empregues para atenuar este tipo de vulnerabilidade, pois não existem ainda soluções baseadas em software que impeçam este tipo de ameaças.

3.3 Implementações Existentes

Neste momento o estado actual do DNSSEC encontra-se completo e pronto a ser utilizado, com alguns promenores relativamente a questões de privacidade mas que se encontram já em fase de resolução (NSEC3 e assinatura online [25]).

Na fase inicial do desenvolvimento do DNSSEC eram apenas duas as implementações de software com suporte DNSSEC para servidores de nomes (BIND e NSD) e com o passar dos anos o número foi aumentando e existem cerca de 7 implementações, sendo o BIND [26] a ferramenta mais adequada de se utilizar até a data porque é aquela que oferece mais funcionalidades para um desenvolvimento mais eficiente de DNSSEC.

3.4 Concretização e Testes

3.4.1 Hierarquia org.pt assinada

A Figura 3.8 apresenta um excerto da zona da hierarquia org.pt assinada, por meio as extensões de segurança ao DNS, numa simulação com 1000 subdomínios assinados.

Além das ferramentas oferecidas pela versão 9 do BIND (Berkeley Internet Name Domain) para a criação de chaves públicas (*dnssec-keygen*) e de assinaturas digitais (*dnssec-singzone*) dos resource records da zona, foram criados "scripts", isto é, ferramentas de execução que possibilitaram realizar determinadas operações de um modo automatizado, seguindo o modelo padrão de assinatura de zonas utilizado em muitos dos trabalhos relacionados, que proporcionou o desenvolvimento de um ambiente simulado de zonas e sub-zonas assinadas. Foi também crucial a utilização do DiG (Domain Information Groper), uma ferramenta de investigação de sistemas DNS também fornecida pelo BIND, que permite procurar informação DNS via interrogações a servidores de nomes.

```
; File written on Mon Jul  9 06:54:33 2007
; dnssec_signzone version 9.4.1
org.pt.                 28800 IN SOA orpheus.fccn.pt. dbadmin.dns.pt. (
                              2007070801 ; serial
                              21600      ; refresh (6 hours)
                              7200       ; retry (2 hours)
                              2419200    ; expire (4 weeks)
                              28800      ; minimum (8 hours)
                              )
                        28800 RRSIG  SOA 5 2 28800 20070808045433 (
                              20070709045433 12153 org.pt.
                              BA87YCgZlBxdbttpe1qMb2ymzBPZPrcaD592
                              ei1DeGDBOltZpSwB1stxy8CZTe0F1lcRFltx
                              E5BwauqpPtn/e4owhTmoKCtFT25PhFI0dqQ3
                              G5ZzfiXpJiWPAI4TvHm57D3dt7any78CUQqf
                              FvZNFVzi7VI3rZXs2G7etrOX6Mg= )
                        28800 NS     orpheus.fccn.pt.
                        28800 RRSIG  NS 5 2 28800 20070808045433 (
                              20070709045433 12153 org.pt.
                              YOogt0Elq0/Nu9ipZVSTbzMKQ8BeHWCQXV2Y
                              z0ZZ9/KZ2QQ+X5HaNi5w3JsKGtxY++lR4Xe0
                              jQkGHgPz/slNWNx170vonHDjHYSswnZgVlrx
                              n9NzFKxICOFN8PSvWojF532QDkzpLYkXReDy
                              DBXCx2sMScMCd0cj5u5+5lDtgQk= )
                        28800 NSEC   1-dnssec.org.pt. NS SOA RRSIG NSEC DNSKEY

...

1-dnssec.org.pt.  28800 IN NS   orpheus.fccn.pt.
                  28800 IN NS   secundario.fccn.pt.
                  28800 DS      59806 5 1 (
                                B48D84767C072C04B75559FCB521F742CD52
                                887B )
                  28800 DS      59806 5 2 (
                                294970C1D668512F3D357058A57162A76C7E
                                FE962E36506546F1B8AE4A134E5D )
                  28800 RRSIG   DS 5 3 28800 20070808045433 (
                                20070709045433 12153 org.pt.
                                oskQeJRHLJUHcN142Vxg1BD856uePEl0oA4G
                                DDGuOzkz3z+n74i5S8Gr/YlcPD2p1/mGaG77
                                iRiWF65lKnmCy+sc85fvgcXfh0Ef7AfOpZvi
                                OX4t6TNP+kYzEquO5LLSDG0zD14hUbfsuoEQ
                                Lqal66YkGUm2WOrM2l1clhd46hY= )
                  28800 NSEC    10-dnssec.org.pt. NS DS RRSIG NSEC
                  28800 RRSIG   NSEC 5 3 28800 20070808045433 (
                                20070709045433 12153 org.pt.
                                of1XnDbiuuRQpj4wJyCT4mluXJ7QFsHQfwl+
                                ggHwDSKQJvYpxDUn85iDCUhk5Ntu/yUll/xh
                                cwqmbyBKC9+agHDYvuTyLYnQuJqbqdSECneP
                                xCKCIE8JnMLpMdRz919VdGgzPdf3FQSG+jlk
                                fTQ1cRSADuyqOE3pC6MWnKfb/Y8= )
10-dnssec.org.pt. 28800 IN NS   orpheus.fccn.pt.
                  28800 IN NS   secundario.fccn.pt.
                  28800 DS      4852 5 1 (
                                F4A1639C03499EB9C73D6C1FC67FCD8DF02D
                                07F6 )
```

Figura 3.8: Segmento da zona pai assinada (zona org.pt)

Os procedimentos realizados para a obtenção de zonas filhas assinadas em grande número, para fins de estudo estatístico do impacto que esta implementação poderá refletir sobre sistema, tiveram a seguinte sequência:

1º Assinar as zonas filhas (zona de teste dnssec.org.pt)

1. Gerar os pares de chaves ZSK e KSK (Zone Signing Key e Key Signing Key):

   ```
   # dnssec-keygen -a RSASHA1 -b 1024 -r /dev/urandom -n zone dnssec.org.pt
   ZSK: Kdnssec.org.pt.+005+51096

   # dnssec-keygen -r /dev/urandom -f KSK -a RSASHA1 -b 1024 -n ZONE dnssec.org.pt
   KSK: Kdnssec.org.pt.+005+39379
   ```

2. Colocar as chaves públicas na respectiva zona:

   ```
   # cat *.key >> dnssec.org.pt (faz o mesmo que um $include)
   ```

3. Actualizar o número de série da zona

4. Assinar efectivamente a zona filha (dnssec.org.pt):

   ```
   # dnssec-signzone -k Kdnssec.org.pt.+005+39379 dnssec.org.pt Kdnssec.org.pt.
   +005+51096
   ```

Após a assinatura de todas as zonas filhas segue-se a assinatura da zona pai de modo a criar uma cadeia segura ou as chamadas ilhas.

2º Assinar a zona pai (zona org.pt)

1. Gerar os pares de chaves ZSK e KSK:

   ```
   # dnssec-keygen -r /dev/urandom -a RSASHA1 -b 1024 -n ZONE org.pt
   ZSK: Korg.pt.+005+17058

   # dnssec-keygen -r /dev/urandom -f KSK -a RSASHA1 -b 1024 -n ZONE org.pt
   KSK: Korg.pt.+005+10783
   ```

2. Colocar as chaves públicas na respectiva zona:

   ```
   # cat *.key >> org.pt
   ```

3. Actualizar o número de série da zona

4. Assinar a zona pai com a opção -g para incluir keyset dos filhos (org.pt):

   ```
   # dnssec-signzone -r/dev/urandom -g -o org.pt -f org.pt.signed -a -t -k
   Korg.pt.+005+10783
   ```

5. Reiniciar o servidor de nomes com a nova configuração da zona (editar named.conf definindo a KSK da zona org.pt como uma *trusted key*)

```
# cat Korg.pt.+005+10783.key >> named.conf
```

6. Efectuar uma pesquisa (dig) por forma a verificar que a resposta contém a informação DNSSEC da zona, segue o exemplo:

```
dig @193.136.192.3 +dnssec +multiline dnssec.org.pt.
```

3.4.2 Resultados Obtidos

Após a criação de um ambiente simulado de zonas assinadas numa hierarquia também ela assinada foi possível verificar os diversos tempos de resposta consoante a dimensão da zona que era simulada.

Os testes efectuados tiveram em vista a preocupação do impacto do processamento e sobrecarga de memória do serviço, foram simulados ambiente com zonas contendo apenas um único subdomínio assinado, até zonas contendo 1000 domínios.

Dimensão do ficheiro de zona

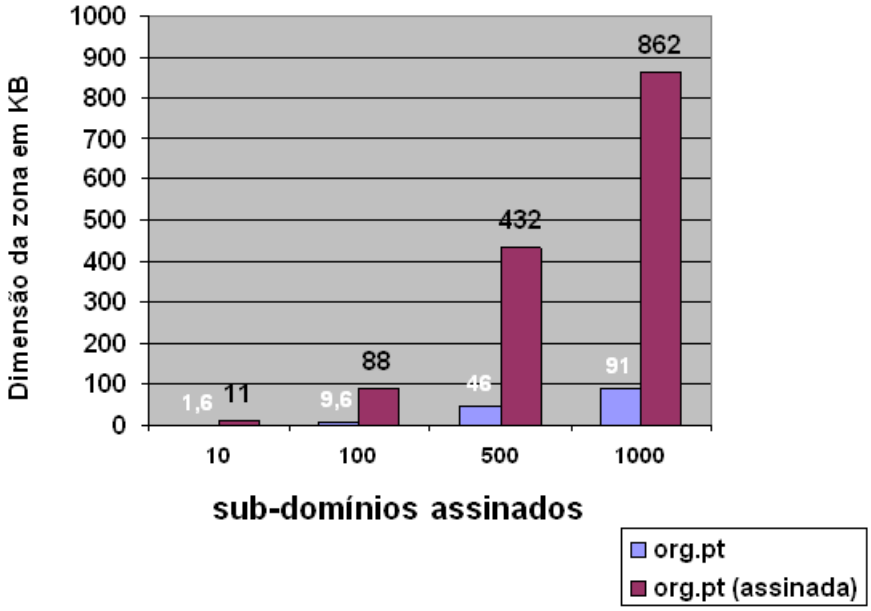

Figura 3.9: Dimensão da zona vs. zona assinada

O presente gráfico da Figura 3.9 tem como objectivo comparar a dimensão de um ficheiro de zona antes e depois de assinado. Foi tomado como exemplo a zona org.pt, que tem actualmente cerca de 500 domínios dos quais apenas 400 se encontram

activos, se todos os domínios activos pretendessem aderir ao DNSSEC o ficheiro de zona org.pt passaria, como se pode ver por análise ao gráfico, de um tamanho de 46 KB para 432 KB, passando o ficheiro actual a ter uma dimensão 10 vezes superior à dimensão inicial antes de assinado.

Apesar do aumento acentuado do tamanho do ficheiro de zona, a unidade em causa são KB (KiloByte), sendo de dimensões ainda irrelavantes para afectar de algum modo o processamento dos servidores de DNS.

Duração do processo de assinatura de uma zona

Foi também realizado um teste comparativo do tempo que uma zona demora a assinar um determinado número de domínios (ver gráfico da Figura 3.10) para que fosse possível observar a capacidade de resposta do servidor de DNS aquando a execução imoderada de domínios assinados.

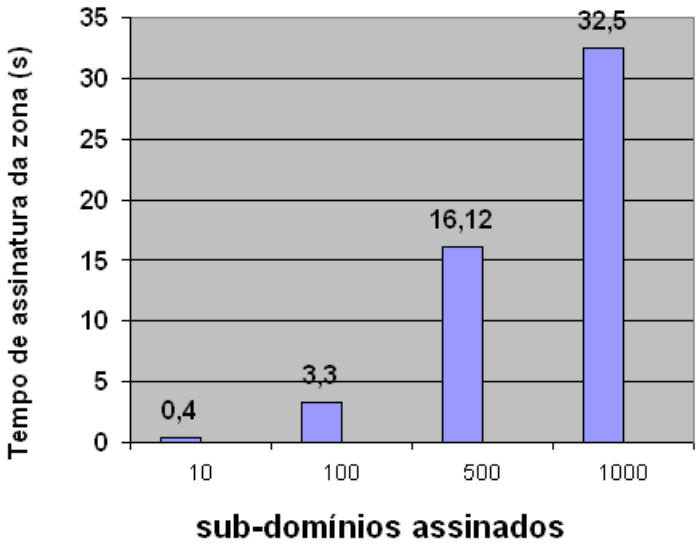

Figura 3.10: Tempo de assinatura de uma zona

Os resultados aqui obtidos foram também bastante positivos pois o tempo de resposta em segundos é pouco significativo com o aumento do número de domínios assinados, existindo quase uma relação de proporção directa entre as variáveis.

Apesar da divergência da dimensão do ficheiro de zona antes e depois de assinado e do tempo de resposta do processo de assinatura pode-se concluir que o número não é preocupante para uma possível entrada em produção, pois as máquinas a suportar estas novas implementações tem uma enorme capacidade de processamento assim como de memória, tendo sido analisado um impacto pequeno em máquinas com menores características é prudente assumir que se irá trabalhar num ambiente com

uma considerável margem de manobra, estando teoricamente ausente de riscos e de falhas de funcionalidades.

Estimativa de Largura de Banda

Foram também efectuados testes com o objectivo de estimar um valor aproximado da largura de banda necessária ao servidor primário de .PT para suportar uma zona .PT completamente assinada.

Através de dados obtidos por meio de uma sonda que analisa o tráfego na rede do servidor primário (ns.dns.pt) foi possível obter as seguintes métricas:

- O tamanho médio das mensagens DNS recebidas pelo servidor primário é de 88 bytes
- O volume de tráfego de DNS que flui de e para o servidor primário tem um valor médio de 11 KB/s

Uma estimativa média do tamanho das mensagens assinadas que irão partir do servidor primário assim que começar a haver zonas com DNSSEC é de 330 bytes.

Estes dados permitem extrapolar que as necessidades de largura de banda imprescindível ao servidor primário de .PT para suportar uma zona .PT completamente assinada é de:

```
11 x 330 / 88 * 8 = 41,25 KB/s
```

Tempo de acesso ao DNS

Outra questão relevante a ter em conta, é a capacidade de resposta do DNS com implementação DNSSEC aos futuros utilizadores, para isso foi realizada uma medição do tempo necessário para aceder ao DNS por parte de um cliente. Através da utilização da ferramenta de gestão do DNS designada por DiG (Domain Information Groper) foi possível medir o tempo de resposta do DNS de domínios assinados.

Após um número considerável de testes foi possível concluir que o tempo de acesso ao DNS de um domínio não varia praticamente nada (variações na ordem de mais ou menos 1 msec), no caso de ter sido efectuada uma interrogação a um domínio assinado com pedido de informação opcional de DNSSEC. No caso de não ser pedida informação opcional o tempo de resposta era exactamente o mesmo.

Na Figura 3.11 segue o resultado do DiG efectuado a um domínio assinado com o comando dig @193.136.192.3 org.pt. +dnssec +multiline que corresponde aos respectivos campos dig @server name +[query options]:

```
; <<>> DiG 9.3.0 <<>> @193.136.192.3 +dnssec +multiline l-dnssec.org.pt.
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6662
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;l-dnssec.org.pt.       IN A

;; AUTHORITY SECTION:
l-dnssec.org.pt.        28800 IN SOA orpheus.fccn.pt. dbadmin.dns.pt. (
                              2007073001 ; serial
                              21600      ; refresh (6 hours)
                              7200       ; retry (2 hours)
                              2419200    ; expire (4 weeks)
                              28800      ; minimum (8 hours)
                              )
l-dnssec.org.pt.        28800 IN RRSIG SOA 5 3 28800 20070808114005 (
                              20070709114005 24381 l-dnssec.org.pt.
                              qILBrlyedAQuDGkfyhdterZXKJvj3eQsgu5TVZFFdAjT
                              b8i2ugFfzUNGCZIWHcGH0yNPHswZgErz9fQl8jKQ50Di
                              /sElECWBqfoXZaDlobdPiiVrA8w0fP4blZsU2ayf9/k4
                              /u72rQ0pF5L2cfT2sbhJFzCW9PxsDct6+o7er00= )
l-dnssec.org.pt.        28800 IN NSEC orpheus.fccn.pt.l-dnssec.org.pt. NS SOA
RRSIG NSEC DNSKEY
l-dnssec.org.pt.        28800 IN RRSIG NSEC 5 3 28800 20070808114005 (
                              20070709114005 24381 l-dnssec.org.pt.
                              mXx4KSAhaKFeq+rKiNJVwYq8AbxUl9QisT3A2x0XVf9j
                              3TtClhgaHtAhJfheRV5RUdLjSF4fDarFaxU/Y+qEPCUq
                              phnwrrF3piHVEv00wGtIXiwlHWQX8kly+0B9ekR9W7Y1
                              kxTXq6FP5YR7hlofC/W0sHN3Ng5uwyXeqPJbRdQ= )

;; Query time: 7 msec
;; SERVER: 193.136.192.3#53(193.136.192.3)
;; WHEN: Mon Jul 30 19:47:05 2007
;; MSG SIZE  rcvd: 509
```

Figura 3.11: DiG realizado a um domínio assinado

O mesmo teste foi realizado para a zona org.pt (ver Figura 3.12) com cerca de 100 domínios assinados e os resultados foram idênticos aos da interrogação DNS de um único domínio, o tempo de acesso ao DNS não modificou em relação ao tempo obtido quando esta não era assinada.

```
; <<>> DiG 9.3.0 <<>> @193.136.192.3 +dnssec +multiline org.pt.
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26972
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1
...
org.pt.                 28800 IN NSEC l-dnssec.org.pt. NS SOA RRSIG NSEC DNSKEY
org.pt.                 28800 IN RRSIG NSEC 5 2 28800 20070808115509 (
                              20070709115509 15021 org.pt.
                              CXXUQDzjBBSz2xn6dqchqY9gAAd2VcZybVxqIzYNaNmw
                              R6lWvBaRSfBDVBzXqTWaKp0+qZ2wADs8HVfi+Wmr34KI
                              vonWf9nm3I9FX0lTdZJ6SqQFKyykd0er3UjyIUuFi8IG
                              LusMH4V2Co6hLpNiT5oKfIXMHm4232L3eFsLiI0= )

;; Query time: 38 msec
;; SERVER: 193.136.192.3#53(193.136.192.3)
;; WHEN: Mon Jul 30 19:30:14 2007
```

Figura 3.12: DiG realizado à zona org.pt

3.5 Integração com o sistema actual

Para que o processo de autenticação dos registos das zonas de um domínio funcione, é necessário haver um ponto de confiança fixado manualmente no cliente ou servidor DNS recursivo e que permita o estabelecimento de uma cadeia hierárquica de autenticação nos subdomínios desse ponto. Esta cadeia de autenticação é obtida através do registo DS na zona pai que é assinada com a sua chave privada.

Esta secção descreve duas formas de actuação possíveis de envio para a zona pai (serviço de registo de domínios .PT) destes registos DS que são gerados pelos administradores das zonas e que permitem uma interacção automática dos administradores dos domínios com o sistema.

3.5.1 Gestão através da interface 'Online'

Figura 3.13: Gestor Online de domínios .PT

Os administradores das zonas devem poder associar, remover, alterar e visualizar os registos DS das zonas que gerem, de forma simples, numa interface web. Para isso pode utilizar-se a interface de criação e gestão de domínios já fornecida aos utilizadores do serviço de registo de domínios, o gestor online de domínios .PT (ver Figura 3.13 [27]). Criando-se um novo menu com informações relacionadas com o novo serviço de segurança no DNS bem como a disponibilização de contactos para

ajuda mais personalizada, os utilizadores poderiam ver as suas questões respondidas e efectuar todos os procedimentos de gestão da sua parte da cadeia de autenticidade das delegações, bem como ser informados quando uma chave estivesse em período de pré-expiração.

3.5.2 Integração no protocolo EPP

O RFC4310 [28] define um método possível para a troca de informação de chaves entre o serviço de registo de domínios e os utilizadores interessados em aderir ao serviço DNSSEC. O EPP (Extensible Provisioning Protocol) é um protocolo XML que permite a interacção directa com o sistema de registo e gestão de domínios e que permite efectuar operações de leitura e escrita sobre os dados que estão sob a gestão do DNS.PT. A flexibilidade deste protocolo permitiu definir facilmente uma forma de comunicar os registos DS através de extensões aos comandos de gestão de nomes de domínios e as mesmas são apresentadas em seguida.

3.5.3 Informação da autenticidade da delegação

O registo DS é publicado pelo servidor DNS para indicar que uma zona filha está assinada digitalmente e que a zona pai reconhece a chave pública indicada na configuração da zona filha como válida. Este registo contém quatro campos: identificador da chave (key tag), número identificador do algoritmo do DNSKEY associado, algoritmo do síntese e a síntese propriamente dita.

A informação de chave pública fornecida por um administrador de zona tem os seguintes campos: sinalizações, protocolo, algoritmo e chave pública.

As assinaturas de chaves e registos DS têm validade e são representadas em segundos.

3.5.4 Comandos EPP

As extensões de DNSSEC ao protocolo EPP permitem efectuar diversas funcionalidades, entre as quais se podem encontrar as seguintes:

- Verificação dos registos DS associados a um domínio (Figura 3.14);
- Associação de registos DS aquando da criação de um domínio (Figura 3.15);
- Alteração de registos DS, útil em trocas de chaves cuja validade está a chegar ao limite ou chaves comprometidas (Figura 3.16);

```
S:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
S:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
S:     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
S:     xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
S:     epp-1.0.xsd">
S:  <response>
S:    <result code="1000">
S:      <msg>Command completed successfully</msg>
S:    </result>
S:    <resData>
S:      <domain:infData
S:       xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
S:       xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0
S:       domain-1.0.xsd">
S:        <domain:name>example.com</domain:name>
S:        <domain:roid>EXAMPLE1-REP</domain:roid>
S:        <domain:status s="ok"/>
S:        <domain:registrant>jdl234</domain:registrant>
S:        <domain:contact type="admin">sh8013</domain:contact>
S:        <domain:contact type="tech">sh8013</domain:contact>
S:        <domain:ns>
S:          <domain:hostObj>ns1.example.com</domain:hostObj>
S:          <domain:hostObj>ns2.example.com</domain:hostObj>
S:        </domain:ns>
S:        <domain:host>ns1.example.com</domain:host>
S:        <domain:host>ns2.example.com</domain:host>
S:        <domain:clID>ClientX</domain:clID>
S:        <domain:crID>ClientY</domain:crID>
S:        <domain:crDate>1999-04-03T22:00:00.0Z</domain:crDate>
S:        <domain:upID>ClientX</domain:upID>
S:        <domain:upDate>1999-12-03T09:00:00.0Z</domain:upDate>
S:        <domain:exDate>2005-04-03T22:00:00.0Z</domain:exDate>
S:        <domain:trDate>2000-04-08T09:00:00.0Z</domain:trDate>
S:        <domain:authInfo>
S:          <domain:pw>2fooBAR</domain:pw>
S:        </domain:authInfo>
S:      </domain:infData>
S:    </resData>
S:    <extension>
S:      <secDNS:infData
S:       xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.0"
S:       xsi:schemaLocation="urn:ietf:params:xml:ns:secDNS-1.0
S:       secDNS-1.0.xsd">
S:        <secDNS:dsData>
S:          <secDNS:keyTag>12345</secDNS:keyTag>
S:          <secDNS:alg>3</secDNS:alg>
S:          <secDNS:digestType>1</secDNS:digestType>
S:          <secDNS:digest>49FD46E6C4B45C55D4AC</secDNS:digest>
S:        </secDNS:dsData>
S:      </secDNS:infData>
S:    </extension>
S:    <trID>
S:      <clTRID>ABC-12345</clTRID>
S:      <svTRID>54322-XYZ</svTRID>
S:    </trID>
S:  </response>
S:</epp>
```

Figura 3.14: Comando EPP: <info>

```
C:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
C:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
C:     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
C:     xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
C:     epp-1.0.xsd">
C:   <command>
C:     <create>
C:       <domain:create
C:        xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
C:        xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0
C:        domain-1.0.xsd">
C:         <domain:name>example.com</domain:name>
C:         <domain:period unit="y">2</domain:period>
C:         <domain:ns>
C:           <domain:hostObj>ns1.example.com</domain:hostObj>
C:           <domain:hostObj>ns2.example.com</domain:hostObj>
C:         </domain:ns>
C:         <domain:registrant>jd1234</domain:registrant>
C:         <domain:contact type="admin">sh8013</domain:contact>
C:         <domain:contact type="tech">sh8013</domain:contact>
C:         <domain:authInfo>
C:           <domain:pw>2fooBAR</domain:pw>
C:         </domain:authInfo>
C:       </domain:create>
C:     </create>
C:     <extension>
C:       <secDNS:create
C:        xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.0"
C:        xsi:schemaLocation="urn:ietf:params:xml:ns:secDNS-1.0
C:        secDNS-1.0.xsd">
C:         <secDNS:dsData>
C:           <secDNS:keyTag>12345</secDNS:keyTag>
C:           <secDNS:alg>3</secDNS:alg>
C:           <secDNS:digestType>1</secDNS:digestType>
C:           <secDNS:digest>49FD46E6C4B45C55D4AC</secDNS:digest>
C:           <secDNS:maxSigLife>604800</secDNS:maxSigLife>
C:           <secDNS:keyData>
C:             <secDNS:flags>256</secDNS:flags>
C:             <secDNS:protocol>3</secDNS:protocol>
C:             <secDNS:alg>1</secDNS:alg>
C:             <secDNS:pubKey>AQPJ////4Q==</secDNS:pubKey>
C:           </secDNS:keyData>
C:         </secDNS:dsData>
C:       </secDNS:create>
C:     </extension>
C:     <clTRID>ABC-12345</clTRID>
C:   </command>
C:</epp>
```

Figura 3.15: Comando EPP: <create>

```
C:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
C:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
C:     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
C:     xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
C:     epp-1.0.xsd">
C:   <command>
C:     <update>
C:       <domain:update
C:        xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
C:        xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0
C:        domain-1.0.xsd">
C:         <domain:name>example.com</domain:name>
C:       </domain:update>
C:     </update>
C:     <extension>
C:       <secDNS:update urgent="1"
C:        xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.0"
C:        xsi:schemaLocation="urn:ietf:params:xml:ns:secDNS-1.0
C:        secDNS-1.0.xsd">
C:         <secDNS:chg>
C:           <secDNS:dsData>
C:             <secDNS:keyTag>12345</secDNS:keyTag>
C:             <secDNS:alg>3</secDNS:alg>
C:             <secDNS:digestType>1</secDNS:digestType>
C:             <secDNS:digest>49FD46E6C4B45C55D4AC</secDNS:digest>
C:           </secDNS:dsData>
C:         </secDNS:chg>
C:       </secDNS:update>
C:     </extension>
C:     <clTRID>ABC-12345</clTRID>
C:   </command>
C:</epp>
```

Figura 3.16: Comando EPP: <update>

3.6 Preparação de um Workshop

Com o intuito de alargar e melhorar os meus conhecimentos acerca do desenvolvimento prático das extensões de segurança ao DNS e de dar a conhecer às entidades portuguesas interessadas (ver Figura 3.17) as vantagens da adesão a este protocolo, tive a oportunidade de preparar um Workshop de DNSSEC no decorrer da 28º Conferência Internacional Pública do ICANN em Lisboa organizada pela FCCN.

Figura 3.17: Convite de participação no Workshop

Por meio de conversações, dois dos formadores de DNS do RIPE NCC com o qual tinha já tido contactado anteriormente, colocaram-se ao dispor para prestar os seus serviços na qualidade de formadores de DNSSEC e em conjunto foi-nos possível organizar um Workshop que teve como principais objectivos dotar os participantes de toda a informação necessária sobre o DNSSEC, os tipos de ataques que este protocolo protege e fornecer experiência prática em como configurar uma zona assinada num

ambiente de referência (BIND).

Os participantes puderam utilizar TSIG [7] para assegurar as transferências entre zonas, assim como assinar uma árvore DNS completa e configurar um resolver para testar a árvore DNS assinada.

Além da experiência prática em DNSSEC, o Workshop também focou as questões operacionais provocadas pela implementação do DNSSEC e foram discutidos os procedimentos específicos implementados pelo RIPE NCC para assegurar as zonas in-addr.arpa.

Foi com grande agrado que participei neste workshop, revelando-se de grande utilidade para o desenvolvimento do projecto, pois a troca de informação e de experiência nos desenvolvimento tecnológicos actuais são uma mais valia para os desenvolvimentos tecnológicos futuros, devo referir que, não obstante, não houve grande adesão por partes das entidades convidadas, o que se deve provavelmente ao facto de se tratar de um assunto ainda em estudo e pouco divulgado.

Capítulo 4

Sumário e Conclusões

Este trabalho, realizado no âmbito do Projecto de Engenharia Informática da FCUL, permitiu conhecer um ambiente institucional que aposta numa grande vertente académica aliada à investigação científica e perspectivar uma carreira profissional aliciante e intimamente ligada ao desenvolvimento e investigação científico e tecnológico.

Em termos pessoais foi muito enriquecedor e entusiasmante porquanto permitiu dar o meu modesto contributo no âmbito do sistema de nomes de domínio de .PT e numa área da engenharia informática que se reveste de grande interesse para todos os intervenientes da comunidade Internet pois aborda e encontra respostas para uma temática de enorme relevância: a segurança nas comunicações.

Em seguida são apresentadas as conclusões obtidas do trabalho realizado bem como uma análise dos passos necessários para a implementação definitiva e estável do DNSSEC no Serviço de Registo de Domínios sob .PT.

4.1 Conclusão

O DNS é um serviço básico da Internet cuja principal utilidade se prende com a atribuição de nomes de domínio a endereços IP sendo este princípio relativamente estável. As vulnerabilidades do protocolo DNS como inicialmente concebido são bem conhecidas e ao longo dos tempos têm sido a base de muitas acções maliciosas direccionadas aos mais diversos serviços da rede.

Face a esta realidade, as extensões de segurança ao protocolo foram sendo desenvolvidas e testadas sem garantia de qualidade de serviço, com algumas implementações práticas que permitiram a sua melhor adopção à realidade da Internet. Este conjunto de extensões encontra-se agora na sua segunda versão e já com vista a uma nova alteração de padrões num dos conceitos em que assenta.

Um estudo de outras implementações e casos práticos de outros Registries (Entidades gestoras do registo de nomes de domínios) permitiu tomar conhecimento dos maiores obstáculos técnicos e administrativos à sua adopção no imediato, deixando o desejo de se iniciar uma fase de testes e implementação piloto no ccTLD .PT.

Dos testes efectuados não resultaram dados que aconselhassem o não avanço da implementação e entrada em produção.

Para que o trabalho de análise e preparação para a entrada em produção ficasse completo não poderia deixar de faltar o capítulo sobre a integração das extensões de segurança com o sistema de registo actual e os moldes em que os administradores de zonas poderão no futuro aceder à gestão dos novos registos definidos nessas mesmas extensões.

4.2 Trabalho Futuro

Ainda não existe uma grande pressão por parte das entidades relevantes que pretendam usufruir do serviço de segurança no DNS a nível global. No entanto, todos os desenvolvimentos nesta área irão ser acompanhados e adoptados assim que se verificar a sua mais-valia real para o combate às vulnerabilidades do DNS.

A entrada em produção deste serviço no DNS.PT será efectuada de forma gradual, começando primeiro pelas hierarquias de .PT, e só depois de se verificar que a sua adopção e integração no sistema está estável é que se poderá tomar a decisão de abrir o serviço a todos os administradores de zonas .PT que assim o entendam.

Por fim, deverão ser efectuadas algumas campanhas de sensibilização para esta temática da segurança na Internet, junto dos Agentes de Registo bem como a sua divulgação pelos media.

Tendo em vista as recomendação dadas por Steve Crocker aquando o acontecimento do ICANN Lisboa 2007, num pequeno encontro com a área técnica do DNS.PT, para que o DNSSEC se propague de um modo exponencial a nível nacional é necessário ter o apoio dos nossos maiores registrars (entidades de registro) e sensibilizando-os para o impacto do constante desenvolvimento da Internet e a crescente preocupação a nível de segurança, deverão ser incentivados adoptar o uso deste protocolo e por consequência os seus clientes também.

De acordo com os estudo que Steve Croker nos revelou, com a adesão de 3 a 4 dos principais registrars de domínios .PT será possível alargar o protocolo DNSSEC a quase 40% da nossa comunidade, e os restantes 60% lhes seguirão.

Acrónimos

BIND	*Berkeley Internet Name Domain* - Programa muito utilizado por servidores DNS
ccTLD	*Country Code Top Level Domain* - Domínio de topo de um país. ".PT" é um exemplo de um ccTLD
DNS	*Domain Name System* - Serviço de nomes da Internet
DNS.PT	Serviço de registo de nomes sob .PT
DNSSEC	*Domain Name System Security Extension* - Conjunto de extensões que aditam segurança ao DNS
Domínio de Topo	Termo genérico que designa gTLDs e ccTLDs que existem sob a raiz da hierarquia de nomes de domínios
EPP	*Extensible Provisioning Protocol* - Protocolo de comunicação normalizado que pode ser utilizado em vários ambientes de gestão de objectos num repositório
Espaço de nomes	Conjunto de valores que podem ser atribuídos a um nó específico da hierarquia de nomes de domínios
Hash	síntese ou resumo criptográfico
host	Servidor de nomes DNS
IANA	*Internet Assigned Numbers Authority*
ICANN	*Internet Corporation for Assigned Names and Numbers*
IETF	*Internet Engineering Task Force* - Grupos de Investigação e Desenvolvimento da Internet
IP	*Internet Protocol* - Protocolo de Internet utilizado entre duas máquinas em rede para encaminhamento dos dados
IPv6	Internet Protocol versão 6

KSK *Key Signing Key* - Chave que assina outra chave

NS *Name Server* - Servidor de Nomes trata-se do servidor responsável por traduzir nomes de domínios e endereços de IP

Online Sistema de gestão online do serviço de registo de domínios sob .PT

Registrar Entidade que fornece o serviço de registo de nomes de domínios a clientes e que serve como intermediário do *Registry*

Registry Entidade que gere o registo de nomes de domínios e possui o repositório oficial da informação. É responsável pela publicação e distribuição dos ficheiros de zona utilizados no sistema de nomes de domínios

RRs *Resource Records* - registos que contém informação relativa a um domínio

RSA *Rivest-Shamir-Adleman* - algoritmo criptográfico de segurança

TLD *Top Level Domain* - Ver descrição para domínio de topo

Zona Conjunto completo da informação para uma determinada sub-árvore do espaço de nomes

ZSK *Zone Signing Key* - Chave que assina a zona

Bibliografia

[1] P. Mockapetris. *RFC 1034: Domain Names - Concepts and Facilities*. IETF, 1987. http://www.ietf.org/rfc/rfc1034.txt.

[2] *DNSSEC Deployment Initiative*. http://www.dnssec-deployment.org/.

[3] *Portal DNS.PT*. http://www.dns.pt.

[4] *Fundação para a Computação Científica Nacional*. http://www.fccn.pt.

[5] *DNSSEC.net*. http://www.dnssec.net.

[6] D. Eastlake. *RFC 2535: Domain Name System Security Extensions*. IETF, 1999. http://www.ietf.org/rfc/rfc2535.txt.

[7] D. Eastlake, O. Gudmundsson, P. Vixie, and B. Wellington. *RFC2845: Secret Key Transaction Authentication for DNS (TSIG)*. IETF, 2000. http://www.ietf.org/rfc/rfc2845.txt.

[8] *Net::DNS*. http://www.net-dns.org/.

[9] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. *RFC 4033: DNS Security Introduction and Requirements*. IETF, 2005. http://www.ietf.org/rfc/rfc4033.txt.

[10] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. *RFC 4034: Resource Records for the DNS Security Extensions*. IETF, 2005. http://www.ietf.org/rfc/rfc4034.txt.

[11] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. *RFC 4035: Protocol Modifications for the DNS Security Extensions*. IETF, 2005. http://www.ietf.org/rfc/rfc4035.txt.

[12] *DNSSEC(.se)*. http://dnssec.nic.se/.

[13] *DNSSEC(.se) Press releases*. http://www.net-dns.org/.

[14] *Registro de Domínios para a Internet no Brasil*. http://www.registro.br/.

[15] Jaime Dias. *Segurança de Aplicação - DNSSEC*. FEUP, 2005/2006. http://web.fe.up.pt/ jaime/0506/SSR/SSR.htm.

[16] M. Andrews. *RFC4431: The DNSSEC Lookaside Validation (DLV) DNS Resource Record*. IETF, 2006. http://www.ietf.org/rfc/rfc4431.txt.

[17] D. Eastlake. *RFC2931: DNS Request and Transaction Signatures (SIG(0)s)*. IETF, 2000. http://www.ietf.org/rfc/rfc2931.txt.

[18] R. Atkinson and S. Kent. *RFC2401: Security Architecture for the Internet Protocol*. IETF, 1998. http://www.ietf.org/rfc/rfc2401.txt.

[19] D. Eastlake. *RFC2537: RSA/MD5 KEYs and SIGs in the Domain Name System (DNS)*. IETF, 1999. http://www.ietf.org/rfc/rfc2537.txt.

[20] D. Eastlake. *RFC2539: Storage of Diffie-Hellman Keys in the Domain Name System (DNS)*. IETF, 1999. http://www.ietf.org/rfc/rfc2539.txt.

[21] D. Eastlake. *RFC2536: DSA KEYs and SIGs in the Domain Name System (DNS)*. IETF, 1999. http://www.ietf.org/rfc/rfc2536.txt.

[22] D. Eastlake. *RFC3110: RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS)*. IETF, 2001. http://www.ietf.org/rfc/rfc3110.txt.

[23] P. Vixie. *RFC2671: Extension Mechanisms for DNS (EDNS0)*. IETF, 1999. http://www.ietf.org/rfc/rfc2671.txt.

[24] R. Arends, B. Laurie, and G. Sisson. *draft-ietf-dnsext-nsec3-11: DNSSEC Hashed Authenticated Denial of Existence*. IETF, 2007. http://www.ietf.org/internet-drafts/draft-ietf-dnsext-nsec3-11.txt.

[25] S. Weiler. *RFC4470: Minimally Covering NSEC Records and DNSSEC On-line Signing*. IETF, 2006. http://www.ietf.org/rfc/rfc4470.txt.

[26] Paul Albitz and Cricket Liu. *DNS and BIND*. O'REILLY, fourth edition, 2001.

[27] *Gestor Online de domínios .PT*. http://online.dns.pt.

[28] S. Hollenbeck. *RFC 4310: Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)*. IETF, 2005. http://www.ietf.org/rfc/rfc4310.txt.

Apêndice A

Planeamento do Projecto

ID	Task Name	Start	Finish
1	Início do Projecto	Mon 04-09-06	Mon 04-09-06
2	**Processo de Integração;**	**Mon 04-09-06**	**Fri 15-09-06**
3	Conhecimento de todos os colaboradores e funções desempenhadas;	Mon 04-09-06	Mon 11-09-06
4	Conhecimentos dos serviços fornecidos pela FCCN;	Mon 04-09-06	Mon 11-09-06
5	Contacto com as aplicações utilizadas para o registo e gestão dos domínios	Mon 11-09-06	Fri 15-09-06
6	**Análise do existente**	Mon 18-09-06	Mon 22-01-07
7	Formação Interna para aquisição do conhecimento na administração dos serviços	Wed 25-10-06	Fri 29-12-06
8	Reunião periódica de acompanhamento do projecto e de outras tarefas do grupo de trabalho	Thu 19-10-06	Thu 19-10-06
9	Descrição do protocolo e planeamento	Mon 01-01-07	Mon 08-01-07
10	**Sessão Interna de Apresentação do Protocolo**	**Wed 17-01-07**	**Wed 17-01-07**
11	Análise da situação dos vários países a nível da adopção do DNSSEC	Tue 23-01-07	Mon 12-02-07
12	**Experimentação, colocar em prática utilizando um servidor DNS de testes**	**Tue 13-02-07**	**Mon 09-04-07**
13	Utilização de um servidor DNS de testes	Tue 13-02-07	Mon 26-03-07
14	Estudo do impacto do DNSSEC no desempenho do Sistema	Tue 27-03-07	Mon 09-04-07
15	**Sessão Interna da Apresentação dos Resultados dos Testes**	**Mon 09-04-07**	**Mon 09-04-07**
16	**Configuração da zona de um subconjunto de domínios num servidor em produção**	**Fri 13-04-07**	**Mon 07-05-07**
17	Zonas de domínios de teste	Fri 13-04-07	Fri 20-04-07
18	Testes de desempenho	Mon 23-04-07	Mon 07-05-07
19	**Entrada em produção em pequena escala**	**Tue 08-05-07**	**Fri 25-05-07**
20	Delegação da hierarquia .org.pt segura no primário	Tue 08-05-07	Fri 18-05-07
21	Testes de desempenho	Mon 21-05-07	Fri 25-05-07
22	**Ver possibilidades de entrada em produção num secundário de .PT**	**Fri 01-06-07**	**Fri 06-07-07**
23	Configuração de toda a zona . PT segura mas apenas num secundário	Fri 01-06-07	Fri 15-06-07
24	Testes de desempenho	Mon 18-06-07	Fri 06-07-07
25	**Sessão de finalização do projecto**	**Mon 09-07-07**	**Mon 09-07-07**

Figura A.1: Calendarização das tarefas (Gantt Project)

O planeamento do projecto consistiu na estipulação de determinadas tarefas e no seu cumprimento, mas tal nem sempre é possível e as tarefas por vezes sofrem desvios que podem influenciar todo o projecto e inclusive a sua conclusão. Apesar dos ligeiros contratempos o curso do projecto decorreu dentro do previsto.

Na Figura A.1 é apresentada a tabela das tarefas definidas com as respectivas datas e durações, na Figura A.2 é ilustrado em forma de Mapa de Gantt o encadeamento das mesmas.

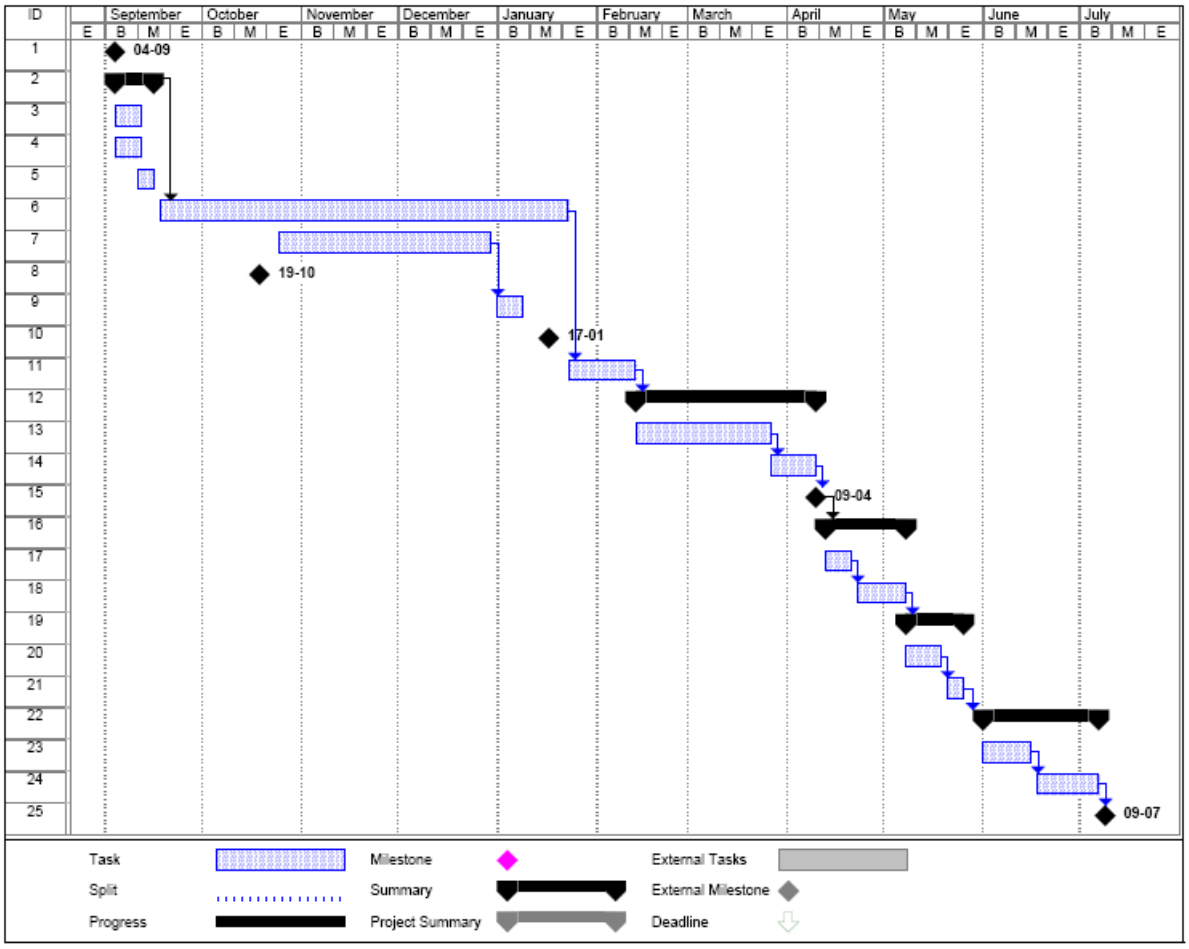

Figura A.2: Mapa de Gantt