



JORNADAS
RCTS
REDE CIÊNCIA, TECNOLOGIA E SOCIEDADE

LISBOA - 9,10,11
DE FEVEREIRO 2010
Grande Auditório
do LNEC - Lisboa

Workshop DNSSEC

Para responsáveis técnicos de
domínios sob .pt

Sara Monteiro

11 de Fevereiro de 2010



Fundação para a Computação Científica Nacional
Foundation for National Scientific Computing





- Conhecimentos de DNS, portátil com ligação à rede por cabo, cliente SSH, configuração DHCP, sistema operativo (X, Mac, Windows)
 - Atendendo ao interesse que o Workshop teve junto dos participantes o que levou a um elevado número de inscritos, o mesmo terá duas sessões, caso o número de participantes na primeira exceda os 20. A nova sessão realizar-se-á no mesmo local, após conclusão da primeira
-
-



- Enquadramento
 - DNS
 - Vulnerabilidades
 - Servidores de nomes
 - Configurações
 - Workshop DNSSEC
 - Configuração da pré-zona
 - Criação de chaves
 - Assinatura da zona
 - Manutenção periódica
-
-



- Rotação das chaves
 - Servidores recursivos
 - Recursos de confiança
 - Ferramentas
 - Desenvolvimentos
 - Documentação
 - Referências
-
-



- O objectivo principal deste workshop é dotar os participantes dos conhecimentos necessários sobre DNSSEC e fornecer experiência prática na configuração e assinatura de zonas DNS num ambiente de referência (BIND).
 - Além da experiência prática em DNSSEC, o workshop também irá focar os tipos de ataque que este protocolo protege e as questões operacionais inerentes à implementação de DNSSEC.
-
-



- Revisão do ano 2008
 - Janeiro: A vida decorria normalmente
 - Fevereiro:
 - Dan Kaminsky descobriu falha grave no DNS e comunicou ao ISC
 - ISC, Microsoft, Cisco e outros fornecedores foram notificados e começaram a trabalhar na actualização das suas ferramentas
 - Julho:
 - Dan Kaminsky “acidentalmente” comunicou a falha à comunidade internet
 - Acompanhamento do CERT – VU#800113
-
-



- Agosto: OMB (*Office of Management and Budget*) lançou o memorando M-08-23 obrigando o desenvolvimento de DNSSEC para o gTLD .gov

 - 2010
 - Actualmente:
 - .gov está assinado
 - .org está em fase de teste
 - .pt está assinado
 - “.” (root) está a fase de testes e assinará oficialmente em Julho de 2010
 - Desde então a normalidade ainda não se voltou a restabelecer...
-
-



- Global, distribuído, fracamente coerente, escalável, bases de dados dinâmicas
 - Comprometido por três componentes:
 - “Espaço de nomes”
 - Servidores colocando disponível esse espaço
 - *Resolver* (clientes) que questionam os servidores acerca do espaço de nomes
 - Base de dados que faz o mapeamento de domínio para endereços IP
 - www.dnssec.pt → 193.137.196.33
 - A BD também contém o mapeamento inverso
-



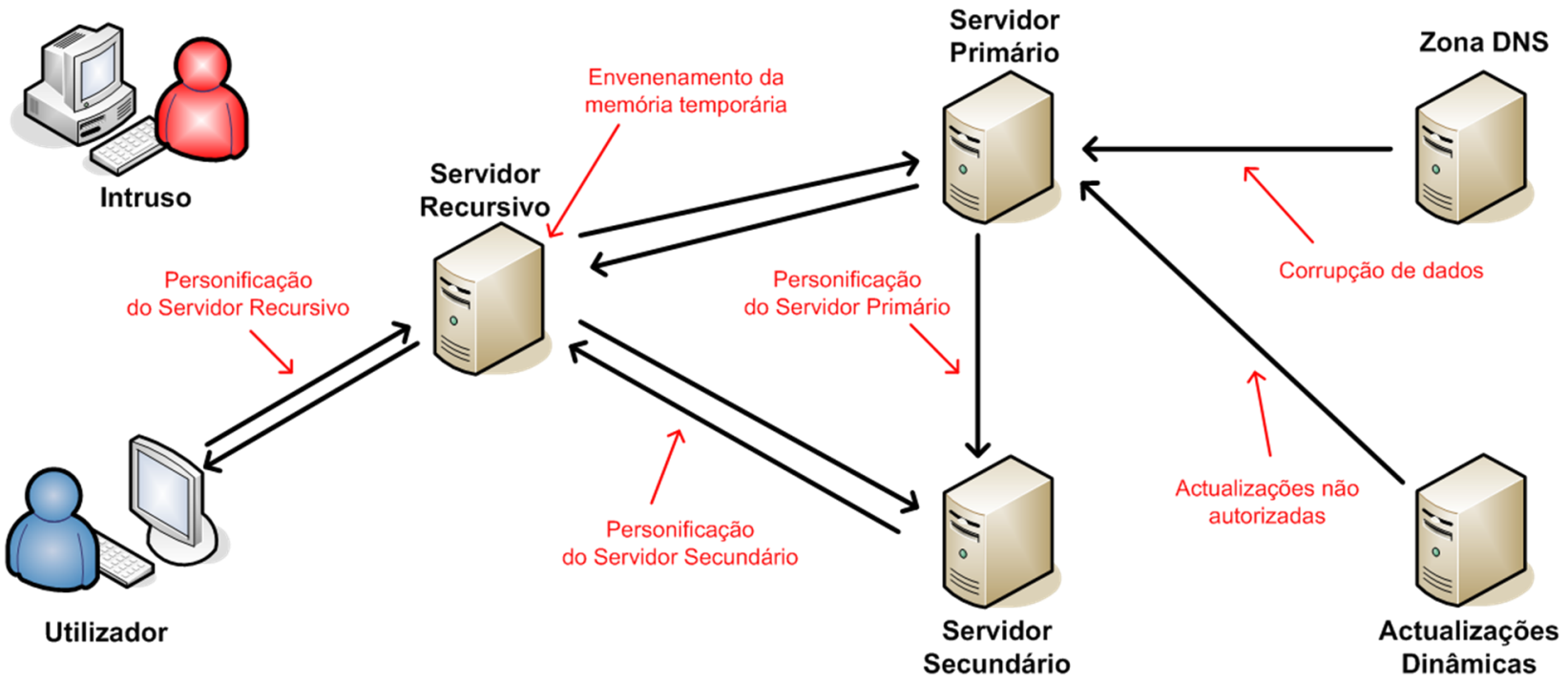
- Coerência:
 - A base de dados interna é consistente:
 - Cada componente (zona) tem um número de série
 - Os número de série são incrementados quando os dados são alterados
 - Alterações na base de dados primária é replicada para as secundários
 - Os dados em memória temporária expiram de acordo com os *timeouts* (TTL) configurados pelos administrados desses dados
 - Não existe limite do tamanho da zona
 - Não existe limite do número de *queries*
-
-



- DNS utiliza UDP e TCP
 - A BD pode ser actualizada dinamicamente
 - Adicionar/apagar/alterar qualquer *resource record*
 - Apenas o servidor primário o permite
 - Espaço de nomes hierárquico
 - Administradores podem criar subdomínios
 - A responsabilidade dos subdomínios pode ser delegada a qualquer outra pessoa que fica responsável pela zona do subdomínio
 - A zona *parent* retém um ligação para as zonas *child* por meio de delegações
-



Vulnerabilidades





- Respondem a *queries* DNS
 - Tipos
 - Autoritário:
 - *master* (primário)
 - *slave* (*secundário*)
 - Servidores recursivos (*caching*)
 - Servidor combinado (autoritário e recursivo)
-
-



- *Master*
 - Autoritário para uma ou mais zonas
 - Zonas são carregadas do disco
 - Respondem a pedidos de transferência de zona
 - Aquando a realização de alterações da zona enviam notificações para os respectivos *slaves*
 - O comando AXFR que é utilizado para realizar uma transferência é realizado por meio de TCP
-
-



- *Slave*
 - Possui dados autoritários para uma ou mais zonas
 - Transfere as zonas do servidor *master*
 - Poderá salvaguarda localmente os dados para o caso de perda do servidor *master*
 - Recebem notificações do *master* para transferência de zona
 - Comparam número de série que lhes é notificado com o da zona que tem carregada e se for anterior ignoram a notificação de transferência
-
-



- Servidor recursivo
 - Realizam a pesquisa concreta do DNS em nome dos seus clientes
 - As respostas são obtidas de servidores autoritários
 - As respostas são armazenadas em memória temporária para futura referência
-
-



- Autoritário vs recursivo
 - Diferença dos papéis de cada um:
 - Autoritário
 - Desconhece os clientes
 - Reconhece as *queries*
 - Recursivo
 - Conhece os clientes
 - Desconhece as *queries*
-
-



- Servidor combinado
 - Podem ter diversos papéis:
 - Autoritário e recursivo
 - Só autoritário mas sendo *master* para algumas zonas e *slave* para outras
 - *Resolver*
 - Envia *queries* em nome das aplicações
 - Normalmente implementado numa biblioteca do sistema (*libc*)
-
-



- BIND

- Por defeito a configuração encontra em *named.conf*
 - A localização da mesma difere consoante o sistema operativo e é configurável na instalação do BIND
 - É dividido em várias secções incluindo:
 - `options {}`
 - Opções que afectam a operação do BIND e de todas as zonas
 - `zone {}`
 - Opções das zonas para o qual o servidor é autoritário ou que são tratadas de forma diferente
 - `logging {}`
 - Gestão e armazenamento dos vários logs produzidos
-
-



- **named.conf**

```
options {  
    directory "etc/namedb";  
    listen-on-v6 { any; };  
    notify yes;  
    pid-file "/var/named/named.pid";  
    dnssec-enable yes;  
    recursion yes;  
    dnssec-validation yes; (para recursivos)  
    ...  
};
```

- Existem muito mais opções:

<http://www.zytrax.com/books/dns/ch7/statements.html>



- `named.conf`
 - É necessário determinar o tipo de zona e configurar as cláusulas que se pretendem:
 - *master/slave/hint...*
- Se for *master*:

<http://www.zytrax.com/books/dns/ch7/zone.html>

```
zone "dnssec.pt" IN {  
    type master;  
    file "primary/signed/dnssec.pt";  
    allow-transfer { 193.137.196.32; };  
};
```



- named.conf

- Se for *slave*:

```
zone "dnssec.pt" IN {  
    type slave;  
    file "slave/dnssec.pt";  
    masters {193.137.196.33; };  
};
```

- O ficheiro de zona tem que ter permissões de escrita para o utilizador que corre o processo BIND
 - No caso de haver múltiplos *masters* o *slave* questiona todos e transfere a zona que tiver o maior número de série
 - Se todos os *masters* têm o mesmo número o *slave* transfere a zona do primeiro *master* que aparece na lista
-



- named.conf

- Se for *hint*:

```
zone "." IN {  
    type hint;  
    file "root.hints";  
};
```

- Desde a versão BIND 9.2 que o ficheiro *root.hints* vem *built in* com o software
-
-



- Ficheiro de zona:
 - Saber a sua localização:

```
etc/namedb/primary/signed/dnssec.pt
```

```
$origin dnssec.pt.  
$TTL 14400      ; 4 hours  
@              IN      SOA      vm07.dns.pt. hostmaster.dns.pt. (  
                2010021101      ; serial  
                14400            ; refresh (6 hours)  
                7200             ; retry (2 hours)  
                604800          ; expire (30 days)  
                300             ; minimum (5 minutes)  
                )  
                IN      NS      vm07.dns.pt.  
                IN      NS      vm06.dns.pt.
```

- Existem diversos tipos de *resource records* e encontram-se definidos no RFC 1034: <http://www.ietf.org/rfc/rfc1034.txt>



– Ambiente do LAB:

- Cada participante tem a uma máquina virtual atribuída
- Todas as máquinas virtuais têm instalado:
 - OpenSSL 0.9.81 5 Nov 2009
 - BIND 9.6.1-P3 built with '--with-openssl' '--prefix=/usr' '--sysconfdir=/etc' '--localstatedir=/var'
- Se falharem as configurações, na pior das hipóteses, devem limpar tudo e recomeçar



– Exercício 1:

- Entrar na respectiva *virtual machine* por ssh

```
# ssh dnssecxx.dns.pt -l admin
```

Nota: **xx** vai de 01 a 22



– Exercício 1:

- Criar e configurar o ficheiro `named.conf`

```
# etc/named.conf
```

- Verificar se a configuração ficou correcta

```
# named-checkconf -z
```

- Configurar o servidor de nomes como autoritário para a zona

```
# zonaxx.dnssec.pt (exemplo: zona01.dnssec.pt)
```

- Verificar se a zona ficou correcta

```
# named-checkzone zonaxx.dnssec.pt zonaxx.dnssec.pt
```



– Exercício 1:

- Trabalhar com outro participante de forma a configurarem os vosso servidor como *slave* para a zona deles e vice-versa
- Não esquecer de reiniciar o named

```
# ps -fax | grep named (para encontrar o pid do named)  
# kill -HUP `named.pid`
```

- Em alternativa se o rndc se encontrar configurado

```
# rndc reload
```



– Exercício 1:

- Verificar se os slaves transferiram com sucesso a zona para o sistema
- Terminem com sucesso verificando a correcta publicação da zona dos servidores autoritativos *master* e *slave*:

```
# dig @dnssecXX.dns.pt zonaXX.dnssec.pt SOA  
(Master)
```

```
# dig @dnssecSS.dns.pt zonaXX.dnssec.pt SOA  
(Slave)
```



– Exercício 2:

- Gerar as chaves que irão assinar a zona
(demora bastante tempo e o resultado é gerado para o ecrã)
 - Fazer cópia de segurança do ficheiro de zona original
 - Incluir as chaves no final do ficheiro de zona
 - Não esquecer de actualizar o número de série para um superior para que os secundários fazem transferência da zona
-
-



– Exercício 2:

- Gerar chaves

- ❖ **ZSK – Zone Signing Key (chave que assina a zona - 256)**

```
# dnssec-keygen -a RSASHA1 -b 1024 -n ZONE zonaXX.dnssec.pt  
Resultado: KzonaXX.dnssec.pt.+005+ZZZZZ
```

- ❖ **KSK – Key Signing key (chave que assina a chave - 257)**

```
# dnssec-keygen -f KSK -a RSASHA1 -b 2048 -n ZONE  
zonaXX.dnssec.pt  
Resultado: KzonaXX.dnssec.pt.+005+KKKKK
```

- Cópia de segurança da zona

```
cp zonaXX.dnssec.pt zonaXX.dnssec.pt.copiaseguranca
```



– Exercício 3:

- Incluir as chaves na zona (zona**xx**.dnssec.pt)

```
$include Kzonaxx.dnssec.pt.+005+zzzzz.key ; ZSK
```

```
$include Kzonaxx.dnssec.pt.+005+kkkkk.key ; KSK
```

- Assinar a zona

```
# dnssec-signzone -k Kzonaxx.dnssec.pt.+005+kkkkk.key
```

```
-o zonaxx.dnssec.pt -t Kzonaxx.dnssec.pt.+005+zzzzz.key
```

- Alterar o nome do ficheiro gerado ou editar o named.conf para conter o ficheiro *.signed

```
# mv zonaxx.dnssec.pt.signed zonaxx.dnssec.pt
```



– Exercício 3:

- Reiniciar o serviço named

```
# kill -HUP "named.pid" (ou rndc reload)
```

- Verificar se a zona ficou bem configurada e responde com DNSSEC

```
# dig @dnssecxx.dns.pt zonaxx.dnssec.pt SOA +dnssec  
+multiline
```



- Sempre que a zona é alterada é necessário ser re-assinada
- As assinaturas da zona tem uma validade por defeito de um mês sendo configurável através opção `-e` do comando `dnssec-signzone`

`-e end-time:`

especifica a data e hora em que os Resource Records RRSIG gerados irão expirar, deve-se indicar um tempo absoluto no formato `YYYYMMDDHHMMSS` (`-e 20101231173000` assinatura válida até 31 de Dezembro de 2010 pelas 17h30m00s). Se não for especificado o `end-time` será configurado por defeito a 30 dias a contar a partir do processo de assinatura, recomendamos que mantenha o formato por defeito para efectuar pelo menos uma manutenção mensal à zona



- Se uma zona não é alterada num espaço de um mês deverá ser forçada uma re-assinatura da mesma não esquecendo de incrementar o número de série



- Deve ser estipulado um mecanismo de rotação de chaves, por exemplo, de 3 a 6 meses no caso da ZSK e 1 a 2 anos a KSK
 - Utilizando força bruta é possível descobrir uma chave de tamanho inferior a 1024 num espaço de 6 meses
 - Por vezes as chaves não são armazenadas de forma segura e são obtidas ilegalmente, o que obriga à necessidade de revogar essas chaves e realizar uma nova geração e rotação das mesmas
-



- Compete aos servidores recursivos a validação DNSSEC
 - Num mundo perfeito os servidores recursivos e *resolvers* apenas terão que confiar nas chaves do “.” (*root*)
 - Quando todas as máquinas passarem a validar DNSSEC, se os domínios tiverem assinados mas a assinaturas tiverem expirado, estes ficarão inacessíveis, isto é, com se tivessem “desaparecido”:
 - Resultados com respostas de SERVFAIL ou REFUSED
-



- Conhecido por trust-anchor
- A validação é feita através de um ponto de confiança, enquanto a *root* não for assinada é possível validar através do DLV do ISC, do ISTAR da IANA ou até de TLDs assinados:

```
trusted-keys {
dlv.isc.org. 257 3 5 "BEAAAAPHMu/5onzrEE7z1egmhg/WPO0+ju
oZrW3euWEn4MxDCE1+lLy2brhQv5rN32RKtMzX6Mj70jdzeND4XknW58
dnJNPCxn8+jAGl2FZLK8t+1uq4W+nnA3qO2+DL+k6BD4mewMLbIYFwe0
PG73Te9fZ2kJb56dhgMde5ymX4BI/oQ+cAK50/xvJv00FrF8kw6ucMTw
FlgPe+jnGxPPEmHAtE/URkY62ZfkLoBAADLHQ9IrS2tryAe7mbBZVcOw
IeU/Rw/mRx/vwwMCTgNbomMQKtUdvNXDrYJDSHZws3xiRXF1Rf+a19UmZ
fSav/4NWLKjHzpT59k/VStTDN0YUuWrBNh";
};
```

(acrescentar no named.conf de um servidor recursivo e manter actualizado)



- Para verificar configurações DNS:
 - [DNSCheck](#) (.se)
 - [DNS for Rocket Scientists](#) (Zytrax)
 - [DNS Reply Size Test Server](#) (OARC)
 - [Updated Reply-Size Tester](#) (RIPE Labs)
 - [Measuring DNS Transfer Sizes - First Results](#) (RIPE Labs)

 - Para validação DNSSEC
 - [Gestor Online de Domínios .PT](#) (DNS.PT)
 - [DNSSEC Look-aside Validation Registry](#) (ISC)
 - [Interim Trust Anchor Repository](#) (IANA)
 - [Open DNSSEC Validating Resolver](#) (OARC)
 - [Verificação de registros DS](#) (Registro.br)
-



- Cada vez existem mais ferramentas com suporte DNSSEC quer a nível de servidores como de aplicações, exemplos:
 - BIND ISC (superior a 9.3.2)
 - NSD, Unbound, ANS, CNS
 - Sparta tools (logwatch, sendmail/postfix/libspf, dnsptkflow...)
 - Mozilla/Firefox/Thunderbird plugins
 - Windows Server 2008 R2 e Windows 7
 - Mais informação em:
 - http://spartatools.dnsops.gov/wiki/index.php/Main_Page
-



- Zona .pt encontra-se assinada e em produção desde o dia 4 de Janeiro de 2010

```
; <<>> DiG 9.6.1-P3 <<>> @149.20.64.21 pt. SOA +dnssec +multiline
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1431
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 8, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;pt.                IN SOA

;; ANSWER SECTION:
pt.                 28747 IN SOA ns.dns.pt. hostmaster.dns.pt. (
                    2010021101 ; serial
                    21600      ; refresh (6 hours)
                    7200       ; retry (2 hours)
                    2592000    ; expire (4 weeks 2 days)
                    300        ; minimum (5 minutes)
                    )
```



- Disponibilizado interface gráfico no sistema online para gestão técnica do DNSSEC:

Gestão de Domínios	Pesquisa Domínio	Registrars	Whois
--------------------	------------------	------------	-------

Gestão de Domínios Online

Processo	Domínio	Hierarquia	Estado	Data Submissão	Facturado até	ET	EG	RA	RT
396741	saramonteiro	.nome.pt	ACTIVE	03/12/2009		S	N	N	S

Consulta: [Ficha de Processo](#)
Opções ET: [Remover Domínio](#) | [Senha p/ alteração EG](#) | [Assumir a Gestão](#) |
Opções RT: [Alterações técnicas](#) | [Pedido de Avaliação](#) | [DNSSEC](#) |

DNSSEC

A tabela que se segue contém informação relativa às chaves associadas ao seu domínio no âmbito da assinatura de domínios por DNSSEC. Para publicar novas chaves, remover chaves anteriormente publicadas ou modificar o estado de chaves referentes à sua zona deverá efectuar aqui as respectivas alterações:

Key Tag	Algoritmo	Tipo	Resumo	Activa	Desde	
28824	7: RSA/SHA-1 (NSEC3)	1	4C15DE1F351C204E31B8D1CE2972E147D05A29C1	Sim	27/01/2010 16:14	<input type="checkbox"/>

Alterações: [Activar](#) [Desactivar](#) [Eliminar](#)



- Disponível em:

<http://www.dnssec.pt>



- <http://www.dnssec-deployment.org>
 - <http://www.dnssec.net>
 - <http://www.root-dnssec.org/>
 - <http://www.net-dns.org/>
 - <http://www.dnssec-tools.org/>
 - http://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions
 - <http://www.ietf.org/dyn/wg/charter/dnsex-charter.html>
 - <http://www.dnssec.net/rfc> (RFCs relacionados)
-



Obrigada pela vossa atenção



<http://www.dnssec.pt>

dev@dnssec.pt | info@dnssec.pt
