Uma Avaliação de Desempenho do DNSSEC

Felipe Gallois Rafael Obelheiro

Grupo de Trabalho de Engenharia e Operação de Redes - 31ª Reunião

13 de maio de 2011

1. Introdução
2. Deficiências do DNS
3. DNSSEC como alternativa de segurança
4. Conclusão

1 Introdução

2 Deficiências do DNS

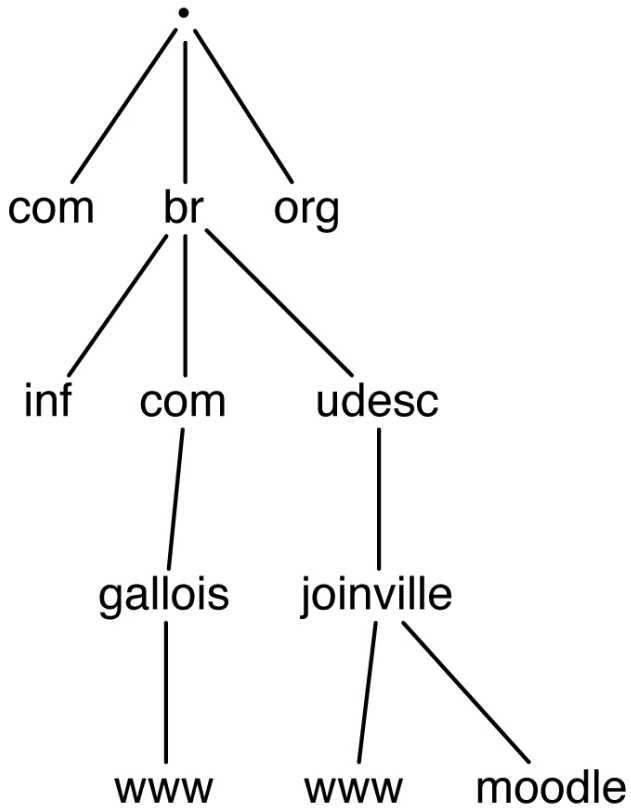
3 DNSSEC como alternativa de segurança

4 Conclusão

O DNS

- DNS (Domain Name System)
  - Um dos pilares da Internet
  - Sistema de diretórios distribuído
  - Usado para mapeamento entre nomes e endereços de computadores na Internet
  - Robusto e descentralizado, suporta grandes cargas
  - **Consideravelmente bem sucedido como um sistema distribuído**
  - Estrutura do espaço de nomes organizada em forma de árvore

Estrutura em árvore do DNS



1 Introdução

2 Deficiências do DNS

3 DNSSEC como alternativa de segurança

4 Conclusão

O Protocolo

- Existem deficiências inerentes ao protocolo, independentes da implementação
- Algumas das vulnerabilidades já são conhecidas há bastante tempo
  - Inexistência de garantia de autenticidade
  - Não há garantia de integridade dos dados
  - Ausência de confidencialidade

Principais consequências

- Redirecionar clientes que fazem uma requisição DNS para algum *host* que não o desejado
- Contaminar o cache de um servidor DNS para que ele responda a requisições com dados incorretos
- Em todos os casos, o *resolver* será redirecionado para um endereço que não corresponde ao nome que solicitou

1 Introdução

2 Deficiências do DNS

3 DNSSEC como alternativa de segurança

4 Conclusão

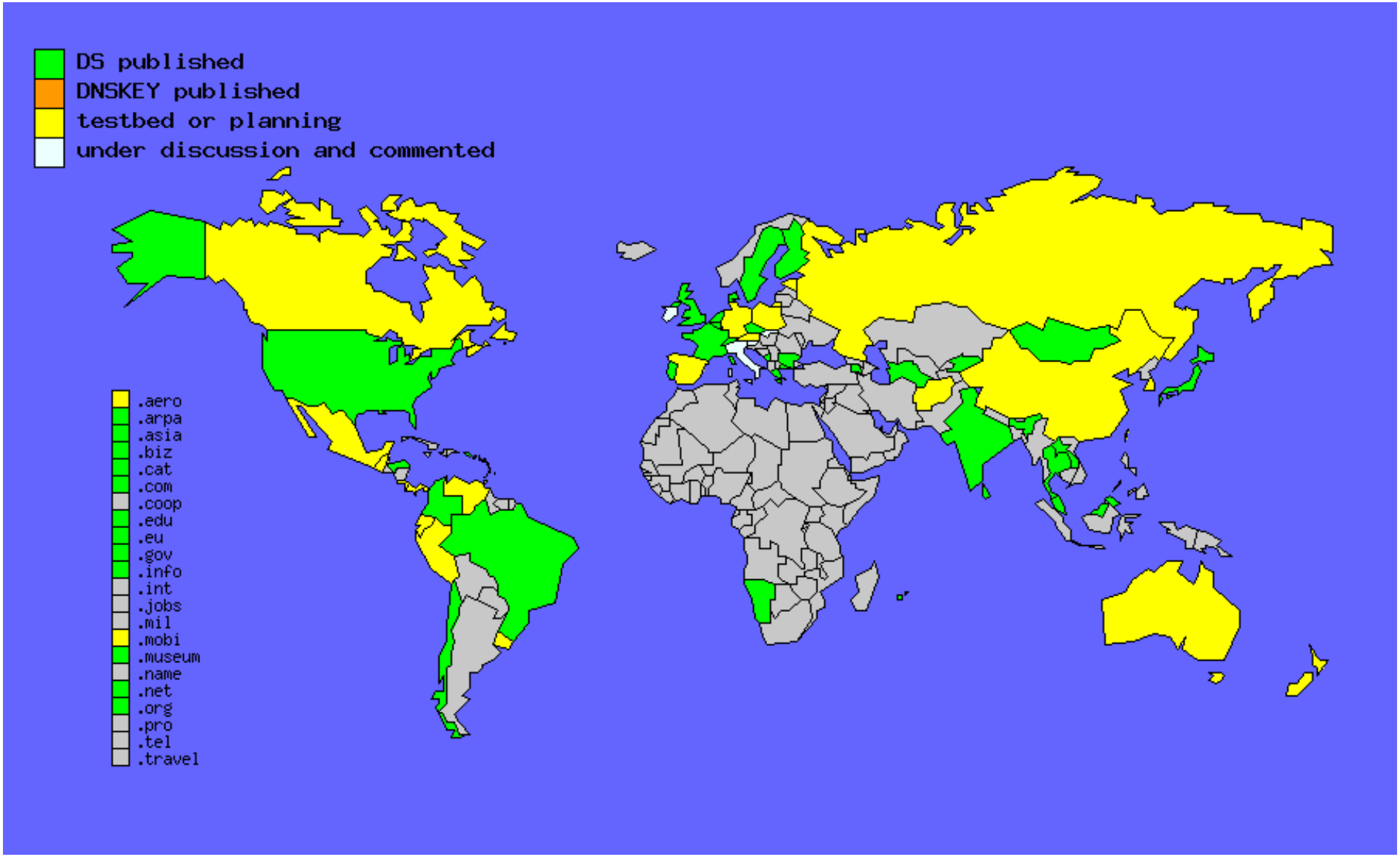
DNSSEC

O DNSSEC oferece uma alternativa de segurança ao DNS:

- Autenticidade de origem
- Integridade dos dados
- Negação de existência autenticada

O estado atual de adoção já é razoavalmente abrangente, com diversos TLDs já oferecendo assinatura de domínios. A assinatura da zona raiz, disponível desde 15 de Julho de 2010, permite que, virtualmente, qualquer domínio possa ser verificado.

Adoção do DNSSEC no mundo



Considerações sobre o DNSSEC

- Apresenta uma série de novos *RRs*
  - DNSKEY
  - RRSIG
  - DS
  - NSEC3
- Existe um custo computacional para se gerar informações que contêm chaves criptográficas, bem como decodificá-las.
- As informações implicam em um tempo adicional de transferência na rede, que pode acarretar em um impacto na utilização do sistema.

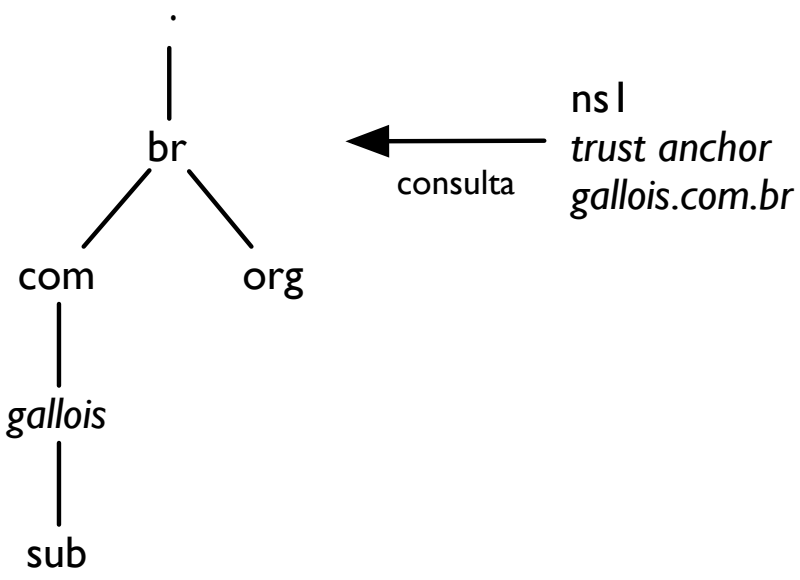
Chaves Criptográficas

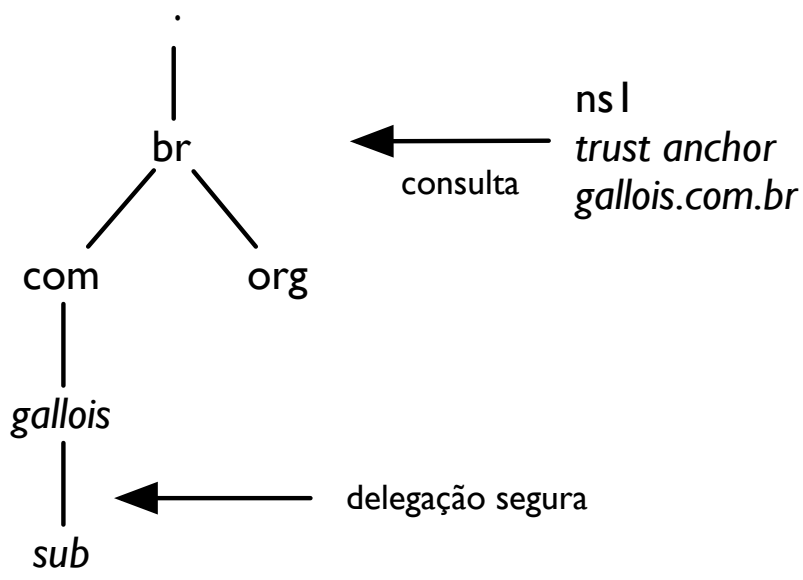
O DNSSEC faz uso de chaves assimétricas (pública e privada).

A chave privada deve ser conhecida apenas por quem assina e a pública distribuída à todos que desejam verificar a informação autenticada.

Os algoritmos criptográficos possíveis para as assinaturas atualmente são: RSA/MD5, DSA/SHA-1, RSA/SHA-1, RSASHA1-NSEC3-SHA1, RSA/SHA-256, RSA/SHA-512 e GOST R 34.10-2001.

Ilhas de Segurança e Cadeias de Autenticação





Preocupação com o desempenho

Como o DNSSEC faz uso de criptografia, então é inevitável uma preocupação com o desempenho do mesmo.

A análise de desempenho foi feita levando em conta três diferentes partes envolvidas na resolução de nomes:

- Servidor autoritativo
- Servidor recursivo
- Cliente

Ambiente de teste

Dois servidores utilizados para os testes:

- VPS Xen Intel Xeon E5405@2.00GHz, com 4 núcleos e 256MB de memória principal. Ubuntu GNU/Linux 10.04. LAN Gigabit, enlace dedicado simétrico de 1Mbps para a Internet.
- Parallels VM Intel Core2 Duo P7350@2.00GHz, 2 núcleos e 136MB de memória principal. Debian GNU/Linux 6.0. LAN Gigabit, enlace de 6Mbps de *download* por 1Mbps de *upload*.

Ferramentas utilizadas

As ferramentas utilizadas para a análise foram as seguintes:

dnssec-tools Utilizada para a geração das chaves e assinatura das zonas.

drill Uma ferramenta baseada no *dig* que conta com algumas alterações para facilitar o uso da mesma com o DNSSEC. Como seu código é aberto, foi possível realizar algumas modificações para que esta se adequasse melhor à análise realizada no trabalho.

dnsperf Usado para avaliar o tempo de resposta de um grande número de consultas DNS, dada uma janela de tempo.

resperf Oferece uma medida direta do *throughput* do servidor.

Servidor autoritativo

Os aspectos considerados ao analisar o desempenho de um servidor autoritativo com DNSSEC foram:

- Tempo de criação de chaves
- Tempo de assinatura de zonas
- *Throughput*

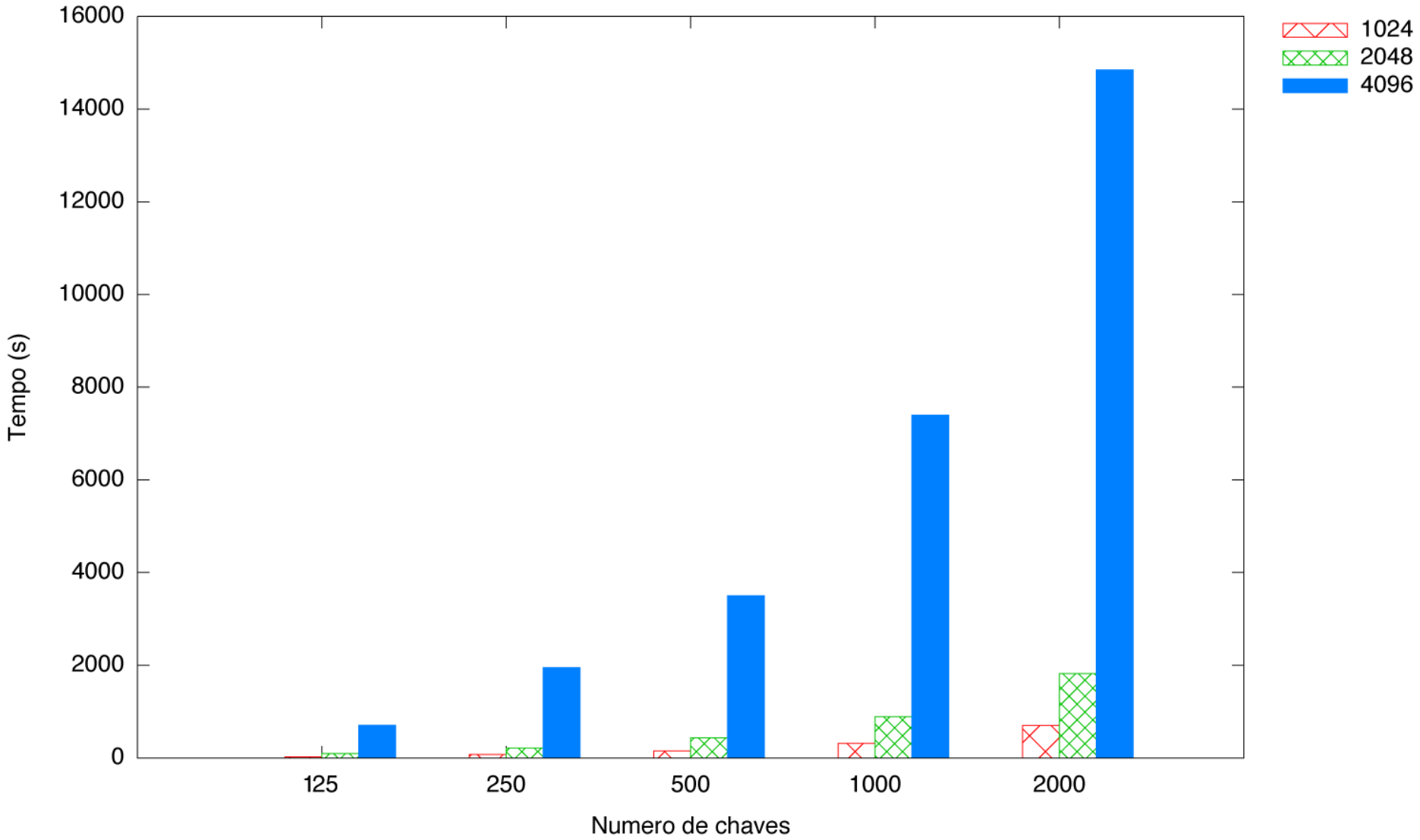
Tempo de criação de chaves

O DNSSEC requer o uso de chaves criptográficas.

Como a criptografia aumenta o custo computacional das operações, é necessário estimar o impacto decorrente.

Foi avaliado o tempo necessário para gerar chaves para um diferente número de zonas e com tamanhos diferentes de chaves.

Tempo de criação de chaves



Tempo de criação de chaves

tamanho (bits)	1024	2048	4096
125 zonas	27,55	93,00	705,57
250 zonas	71,36	212,33	1948,04
500 zonas	154,96	430,26	3498,94
1000 zonas	316,99	889,76	7393,38
2000 zonas	703,71	1817,83	14847,32

Tempo de criação de chaves

Avaliação:

- O tempo de criação de chaves cresce linearmente em função da quantidade de zonas (número de chaves a ser geradas).
- O tempo cresce exponencialmente em relação ao tamanho das chaves criadas.
- O tamanho da zona (quantidade de chaves a ser geradas) dificilmente representa algum impacto em um ambiente real. Um servidor dedicado é capaz de atender à demanda.
- A geração de chaves de 4096 bits é inviável, mesmo para servidores dedicados, uma vez que o tempo exigido por essa tarefa é muito grande para TLDs.

Tempo de assinatura de zonas

A assinatura de zonas é feita para garantir que a autenticidade e a integridade dos dados. Este passo é de suma importância para que o DNSSEC possa efetivamente garantir a segurança que se propõe.

Tempo de assinatura de zonas

Tabela: Total de assinaturas de zonas por segundo

tamanho (bits)	1024	2048	4096
zonas/segundo	218,00	64,37	12,37

Tempo de assinatura de zonas

Avaliação:

- Quantidade de zonas possível de se assinar por segundo diminui exponencialmente em relação ao tamanho da chave utilizada para assiná-la.
- Chaves de 4096 bits para assinar as zonas de um TLD, como o registro.br(registro.br, 2011) com um número de quase 2.5 milhões de zonas, exigiram um tempo inferior a 3 dias.

Throughput

Um aspecto importante referente a servidores autoritativos com DNSSEC é a quantidade de respostas que estes podem oferecer em um determinado período de tempo.

Como o DNSSEC apresenta uma maior quantidade de registros, bem como um um maior tamanho dos mesmos, é importante avaliar se a quantidade de respostas que um servidor pode oferecer é muito prejudicada com a implementação do mesmo.

Throughput

Tabela: Porcentagem de consultas mais rápidas que 10ms e *throughput*

	$\leq$ 10ms(%)	consultas/s
localhost A	98,92	4186
localhost DNSKEY	99,00	3756
foo.eng.br. A	93,97	3992
foo.eng.br.DNSKEY	99,04	3634

Throughput

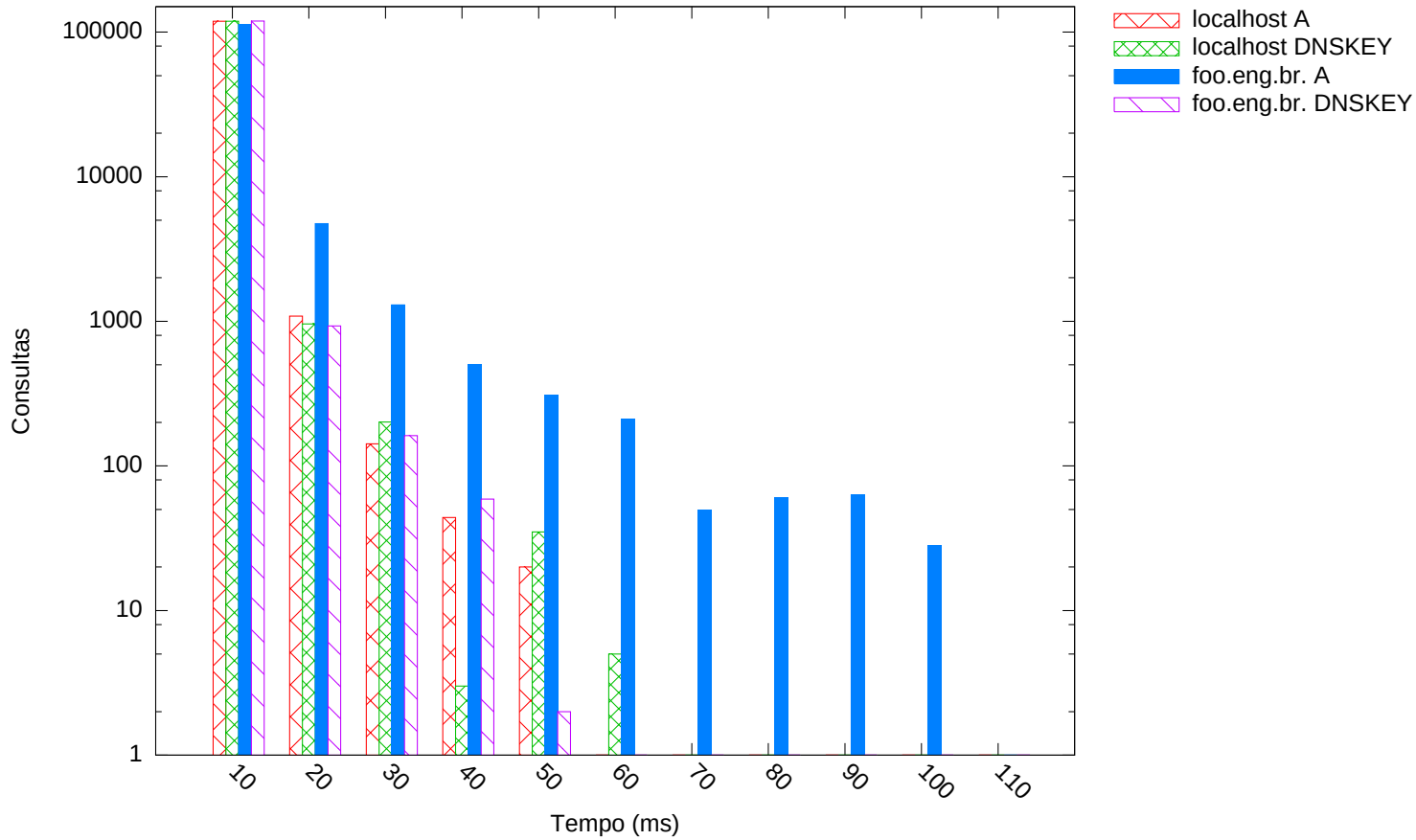


Figura: Tempo de resposta de consultas (eixo y em escala logarítmica)

Avaliação dos resultados em servidores autoritativos

Avaliação:

- O tamanho da chave utilizada, tanto na criação quanto na assinatura, é o fator de maior impacto no desempenho.
- Chaves de até 2048 bits representam um impacto de cerca de 10% no desempenho do servidor.
- A utilização de chaves de mais de 4096 bits inviabilizam a implantação de um servidor DNSSEC.

Servidor recursivo

Para um servidor recursivo, os aspectos analisados para avaliar se o desempenho do mesmo é impactado pelo DNSSEC foram:

- Tempo de validação de cadeia.
- Tempo de consulta sem validação.

Validação de cadeias

O tempo de validação de cadeias foi avaliado de duas maneiras diferentes, uma sem utilizar o *cache* do servidor recursivo e outra utilizando.

O uso do *cache* foi empregado pois este representa uma situação comum nos servidores DNS em ambientes reais.

Foram realizadas 1000 consultas para cada dos seguintes servidores: *foo.eng.br*, *bb.b.br*, *bradesco.b.br*, *cnj.jus.br*, *stf.jus.br*, *b.br*, *eng.br*, *jus.br*, *isc.org*, *br*, *org*, e *"." (raiz)*.

Validação de cadeias DNSSEC sem *cache*

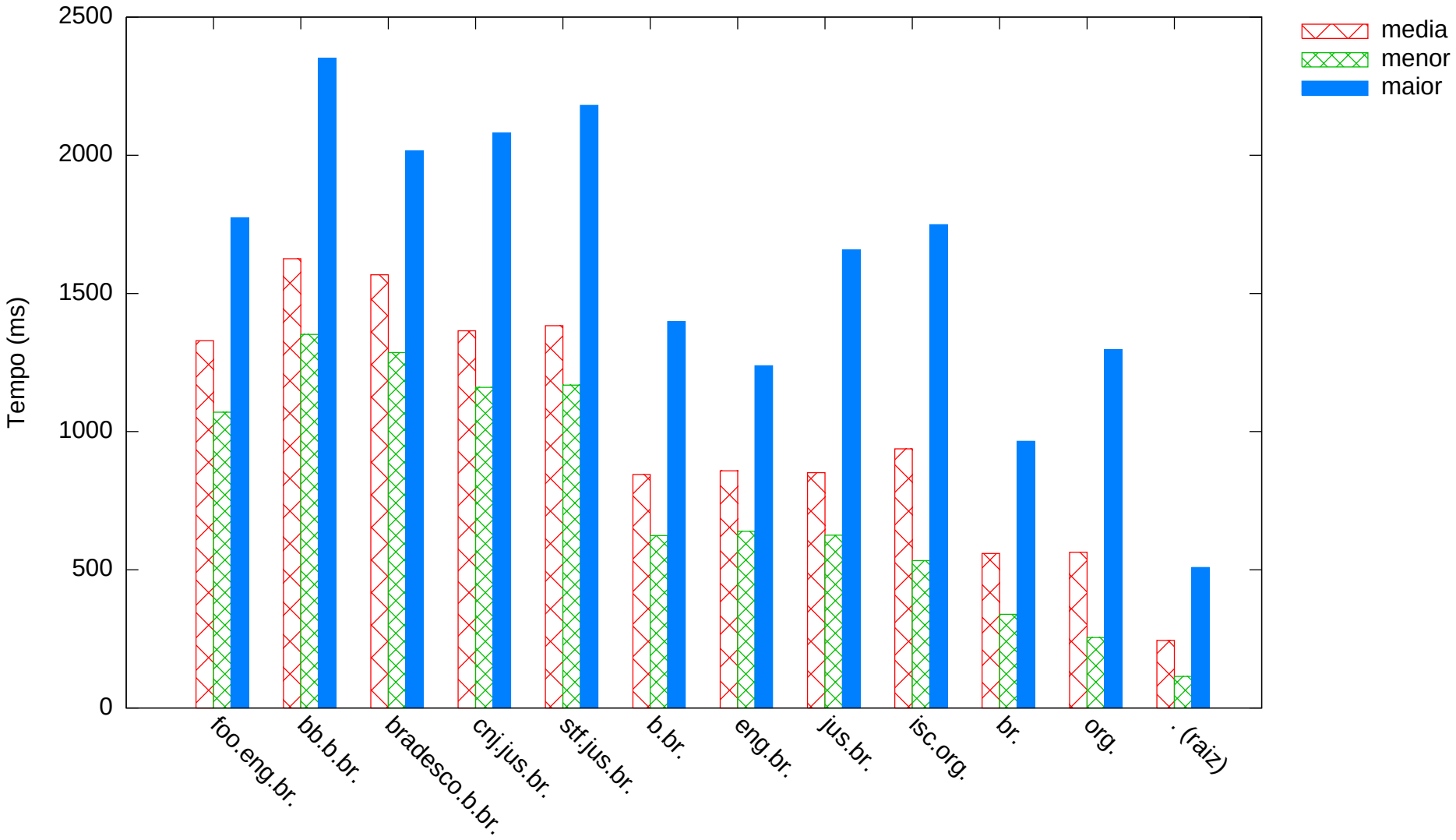


Figura: Tempo de validação de cadeias DNSSEC sem *cache*

Validação de cadeias DNSSEC sem *cache*

Tabela: Tempo de validação de cadeia DNSSEC (sem *cache*)

nome	média (ms)	desvio	níveis
foo.eng.br.	1329,04	123,08	4
bb.b.br.	1625,65	140,55	4
bradesco.b.br.	1567,48	132,05	4
cnj.jus.br.	1364,80	125,92	4
stf.jus.br.	1383,02	140,32	4
b.br.	844,68	128,69	3
eng.br.	858,12	130,41	3
jus.br.	851,38	157,81	3
isc.org.	937,99	195,41	3
br.	559,14	123,40	2
org.	563,53	168,07	2
. (raiz)	244.44	99,19	1

Validação de cadeias DNSSEC com *cache*

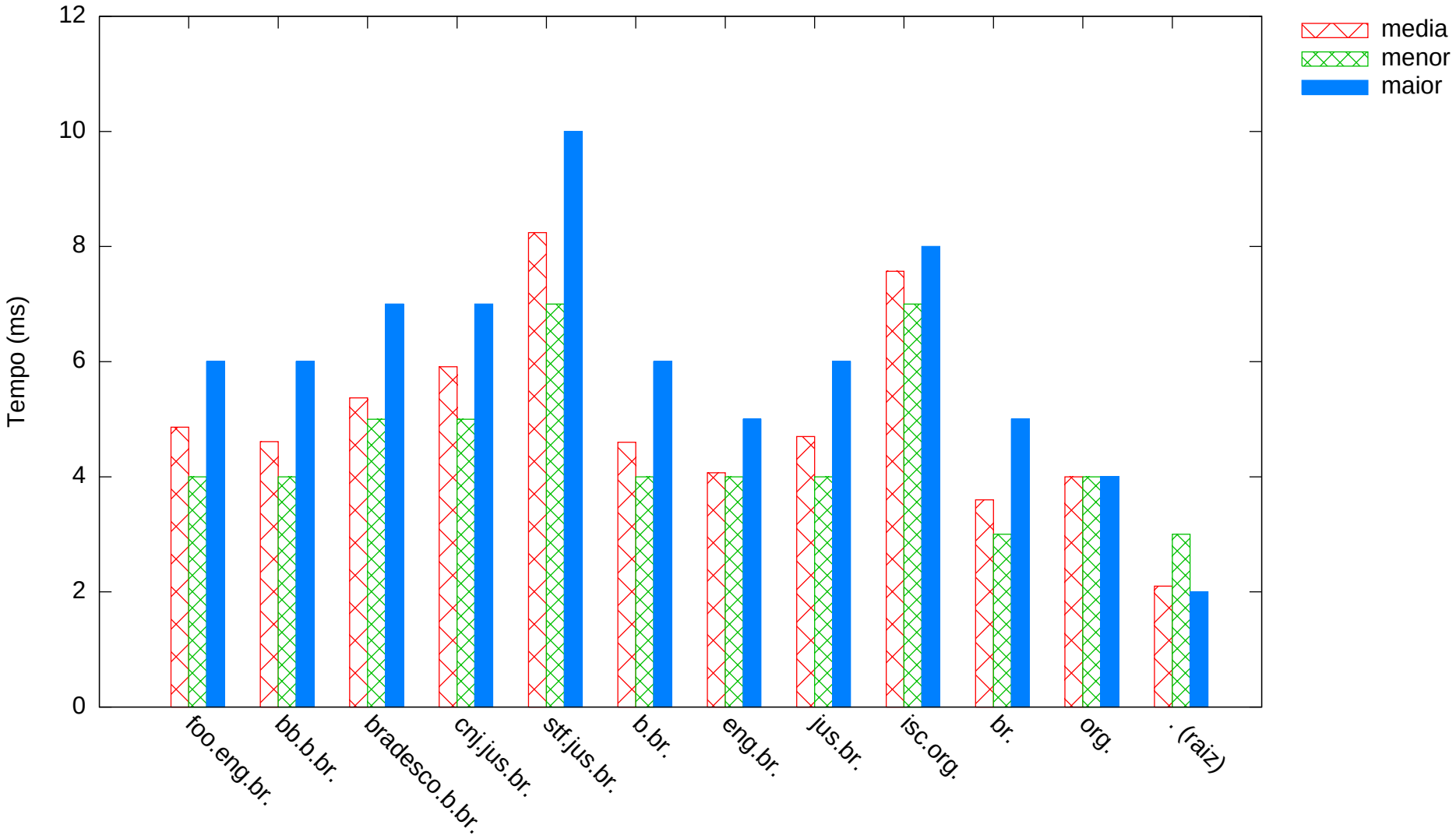


Figura: Tempo de validação de cadeias DNSSEC com *cache*

Validação de cadeias DNSSEC com *cache*

Tabela: Tempo de validação de cadeia DNSSEC (com *cache*)

nome	média (ms)	desvio	níveis
foo.eng.br.	4,86	0,37	4
bb.b.br.	4,61	0,53	4
bradesco.b.br.	5,37	0,50	4
cnj.jus.br.	5,91	0,54	4
stf.jus.br.	8,24	0,52	4
b.br.	4,60	0,50	3
eng.br.	4,07	0,25	3
jus.br.	4,70	0,50	3
isc.org.	7,57	0,50	3
br.	3,60	0,50	2
org.	4,00	0,00	2
. (raiz)	2,10	0,20	1

Consulta DNS sem *cache*

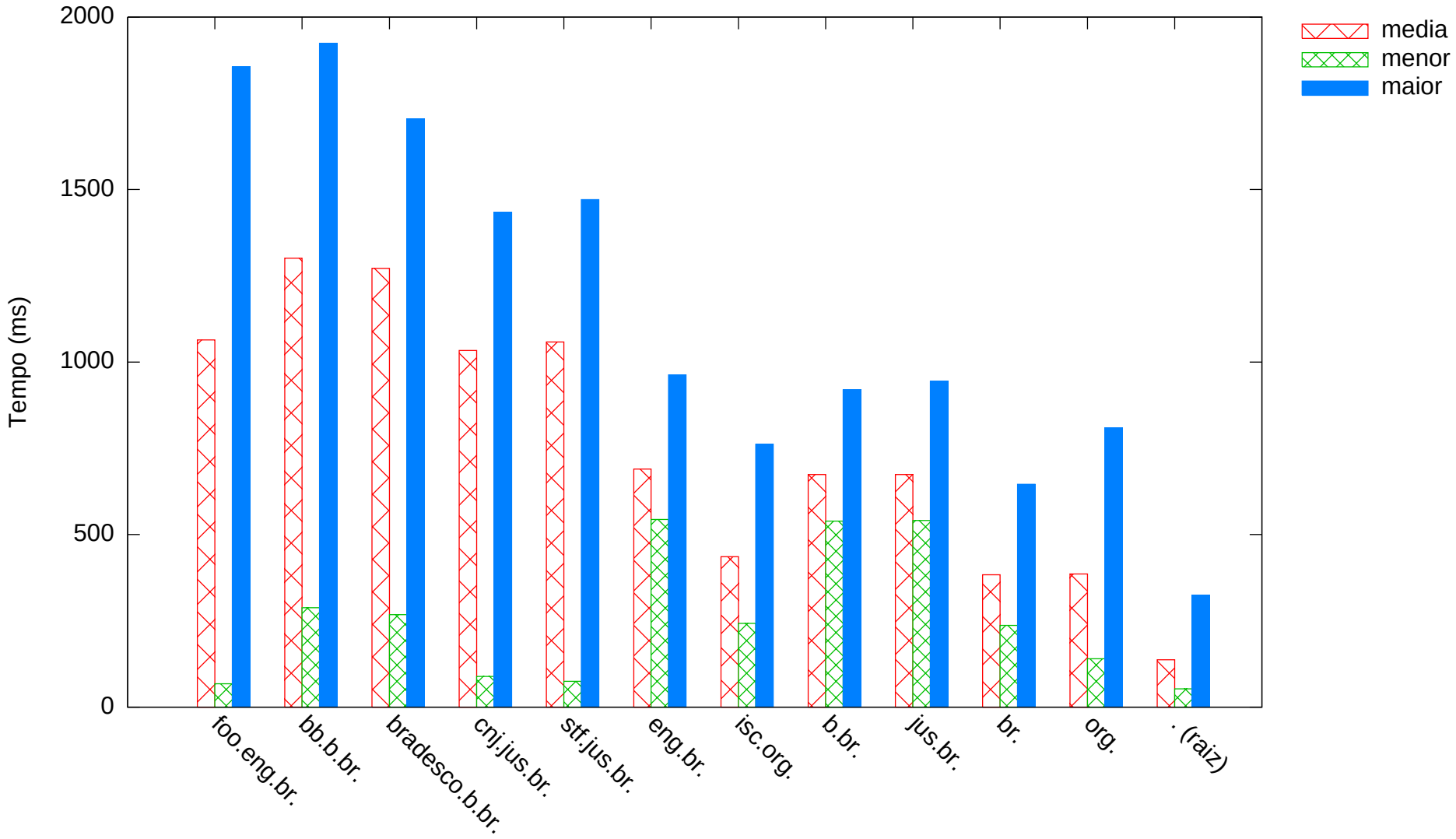


Figura: Tempo de consultas DNS sem *cache*

Consulta DNS sem *cache*

Tabela: Tempo de consulta DNS sem *cache*

nome	média (ms)	desvio	níveis
foo.eng.br.	1064,17	344,85	4
bb.b.br.	1301,14	347,03	4
bradesco.b.br.	1271,38	334,84	4
stf.jus.br.	1058,47	348,04	4
cnj.jus.br.	1033,58	365,87	4
b.br.	674,28	79,28	3
eng.br.	690,29	88,67	3
jus.br.	673,85	82,91	3
isc.org.	436,30	117,90	3
br.	383,87	86,32	2
org.	386,11	136,88	2
. (raiz)	137,30	66,83	1

Consulta DNS com *cache*

O tempo de resposta de consultas DNS com *cache* foi sempre menor ou igual a 1ms, e portanto, para efeitos de comparação, foi desconsiderado.

Avaliação dos resultados em servidores recursivos

Com os resultados obtidos é possível concluir que:

- O tempo total para se obter uma resposta, quando uma consulta é feita sem utilizar *cache*, aumenta em razão da quantidade de níveis do nome.
- O tempo médio de resposta de consultas DNSSEC com *cache* não sofre muita variação e não demonstra estar atrelada ao número de níveis de uma nome.
- O tempo de validação de cadeias sem *cache* é, em média, 30% maior que o tempo uma consulta DNS convencional e 185,15 vezes maior que o tempo de validação com *cache*.

Avaliação dos resultados em servidores recursivos

O tempo necessário para retornar uma consulta DNSSEC utilizando o mecanismo de *cache*, que é uma prática recomendada (Aitchison, 2005), não representa um impacto considerável no desempenho do sistema.

Considerando os dados levantados por Jung, Sit, Balakrishnan e Morris (2002)[1]:

	Taxa de *cache hit*	
	Pior caso (80%)	Melhor caso (87%)
Tempo de resposta (com cache)	20%	17%
Tempo de resposta (sem cache)	41x maior	36x maior

[1] estimativa

Cliente

Na análise do desempenho do DNSSEC por parte do cliente, foram avaliados 5 portais web brasileiros entre os mais acessados de acordo com o *ranking* do Alexa.com em 2010(Alexa, 2010). Os sites analisados foram: *globo.com*, *terra.com.br*, *msn.com.br*, *yahoo.com.br* e *uol.com.br*.

Foram extraídos os nomes de dentro do documento HTML da página principal de cada um destes portais e avaliado o tempo total para a resolução de todos eles utilizando o DNSSEC, com e sem *cache*. Além disso, foi usado o Firebug para calcular o tempo total de carregamento da página e comparar com o tempo de resolução de nomes.

globo.com

níveis de domínio	2	3	4
domínios/nível	2	117	23
DNSSEC (ms)	1746	170118	42715
DNSSEC com *cache* (ms)	10,48	678,6	161,8
total DNSSEC (s)	214,58		
total DNSSEC com *cache* (s)	0,85		
carregamento frio da página (s)	7,51		
carregamento quente da página (s)	4,64		

terra.com.br

níveis de domínio	4	5
domínios/nível	33	2
DNSSEC (ms)	61287	4521
DNSSEC com *cache*(ms)	232,1	16,53
total DNSSEC (s)	65,81	
total DNSSEC com *cache* (s)	0,25	
carregamento frio da página (s)	4,42	
carregamento quente da página (s)	2,45	

msn.com.br

níveis de domínio	2	3	4
domínios/nível	1	7	24
DNSSEC (ms)	873	10178	44572
DNSSEC com *cache* (ms)	5,24	40,6	168,8
total DNSSEC (s)	55,62		
total DNSSEC com *cache* (s)	0,22		
carregamento frio da página (s)	8,78		
carregamento quente da página (s)	7,43		

yahoo.com.br

níveis de domínio	3
domínios/nível	1
DNSSEC (ms)	1454
DNSSEC com *cache* (ms)	5,80
total DNSSEC (s)	1,454
total DNSSEC com *cache* (s)	0,0058
carregamento frio da página (s)	9,22
carregamento quente da página (s)	7,84

uol.com.br

níveis de domínio	4	5
domínios/nível	70	11
DNSSEC (ms)	130003	24864
DNSSEC com *cache* (ms)	492,33	90,93
total DNSSEC (s)	154,87	
total DNSSEC com *cache* (s)	0,58	
carregamento frio da página (s)	14,32	
carregamento quente da página (s)	9,77	

Avaliação dos resultados em clientes

Avaliação:

- O uso de servidores recursivos com *cache* desabilitado refletem em um impacto no cliente que inviabilizam a implantação.
- O uso de *cache*, entretanto, reduz o tempo de resolução de nomes para um valor imperceptível, considerando-se o tempo total de carregamento da página.

1 Introdução

2 Deficiências do DNS

3 DNSSEC como alternativa de segurança

4 Conclusão

Conclusão

A compatibilidade com o DNS e a adoção do DNSSEC por parte dos órgãos que gerenciam os domínios de primeiro nível e a zona raiz oferecem atualmente um cenário favorável para a implantação do último.

O DNSSEC, se consideradas algumas restrições, pode ser utilizado em ambientes de produção sem acarretar em grande impacto no desempenho de ponta a ponta do sistema. É possível, entretanto, que o uso de URLs em páginas web pode representar um impacto perceptível no tempo de carga das mesmas.

A conclusão é, portanto, de que o uso do DNSSEC é totalmente viável desde que corretamente configurado.

Referências

1. AITCHISON, R. **Pro DNS and BIND**. First ed. New York: Apress, 2005. 571 p. ISBN 1-59059-494-0.
2. ALEXA.COM. **Alexa - Top sites in Brazil.** 2010. Disponível em: http://www.alexa.com/topsites/countries/BR. Acesso em: 26/10/2010.
3. BALAKRISHNAN, H.; JUNG, J.; MORRIS, R.; SIT. E. **DNS Performance and the Effectiveness of Caching**. 2002. Disponível em nms.csail.mit.edu/papers/dns-ton2002.pdf
4. GALLOIS, F. **Uma Avaliação de Desempenho do DNSSEC**. 2010. Disponível em: http://www.pergamumweb.udesc.br/dados-bu/000000/000000000010/000010E6.pdf
5. registro.br **ESTATÍSTICAS**. 2011.Disponível em: https://registro.br/estatisticas.html. Acesso em: 09 mai. 2011.

Perguntas?