



DNSSEC

Tester av routrar för hemmabruk

Joakim Åhlund & Patrik Wallström, Februari 2008

Innehållsförteckning

Innehållsförteckning 1

1 Introduktion 2

- 1.1 Detta dokument 2
- 1.2 Förkortningar & ordförklaring 2
- 1.3 Referenser 2
- 1.4 Typsnitt 2
- 1.5 Om .SE 2

2 Introduktion - Routertester 3

- 2.1 Bakgrund 3
- 2.2 Inkluderat och exkluderat 3
- 2.3 Hur 3
- 2.4 Testmiljön 4
- 2.5 Beskrivning av testerna 4

3 Resultatet i sammanfattning 6

- 3.1 Testresultatet 6
- 3.2 Åtgärder 6
- 3.3 Fortsatt arbete 6

4 Bilagor 7

- 4.1 Bilaga 1, DNS test protocol for SOHO-routers 7
- 4.2 Bilaga 2, Resultat från testprotokoll 10

Figurförteckning

- Figur 1: Testmiljö 4

1 Introduktion

1.1 Detta dokument

Detta dokument är en rapport som beskriver resultatet av de tester vi genomfört på bredbandsroutrar för hemmabruk. Syftet har varit att ta reda på i vilken skala dessa produkter har problem med DNSSEC.

1.2 Förkortningar & ordförklaring

Förkort *Förkortning*, detta är en förkortning

1.3 Referenser

[1] Referenser till andra dokument etc.

1.4 Typsnitt

I detta dokument används följande typsnitt:

Liten fetstil Används för biblioteksstruktur, filnamn samt in- och utmatningar.
STORA BOKSTÄVER Datornamn skrivs alltid med stora bokstäver.

1.5 Om .SE

Stiftelsen för Internetinfrastruktur (.SE) ansvarar för Internets svenska toppdomän, .SE. Kärnverksamheten är registrering av domännamn samt administration och teknisk drift av det nationella domännamnsregistret under .se. .SE är en oberoende allmännyttig organisation som verkar för en positiv utveckling av Internet i Sverige. Genom .SE:s Internetfond avsätter stiftelsen varje år medel till projekt som på olika sätt bidrar till Internets utveckling och användning. Se mer på www.iis.se

2 Introduktion - Routertester

2.1 Bakgrund

I september 2007 fick den DNSSEC-signerade domänen gavle.se problem med tillgänglighet. Detta upptäcktes då internetanvändare började höra av sig till kommunen.

Problemen visade sig bero på en kombination av hemmaroutrar och en bugg i programvaran BIND. Namnservrarna som TeliaSonera och Tele2 körde var BIND version 9.4.1, och den versionen satte en flagga (AD-biten) i DNS-protokollet felaktigt. Det som hände med vissa modeller av hemmaroutrar var att DNS-trafiken mot signerade domäner inte fungerade. Gavle.se var den första större domänen som normalt attraherade en större allmänhet, så detta blev ett större test av DNSSEC mot vanliga konsumenter vilket tidigare inte provats i den här skalan.

Dessa problem var alltså resultatet av ett fel i BIND i kombination med fel i vissa konsumentroutrar. Vi insåg att det vi behövde genomföra ordentliga testar av routrar från olika märken för att få en uppfattning om hur utspritt problem av den här karaktären är.

2.2 Inkluderat och exkluderat

En testspecifikation är upprättad, den återfinns i bilaga 1.

Det vi har inriktat oss på i testerna är:

- DNSSEC, både då validering sker av klienten eller i t.ex. ISP:ns resolver
- EDNS0
- DNS-frågor om udda posttyper (AAAA mm)
- Open Recursive Resolver
- AS112-frågor

Det som är exkluderat från testerna är:

- Underliggande protokoll
- Fragmentering av paket

Det kan även vara så att det finns brister i andra funktioner i routrarna, såsom brandvägg eller DHCP, men vi har begränsat oss till DNS.

2.3 Hur

Routrarna som har testats är inköpta hos närmaste/billigaste datorbutik, på samma sätt som en vanlig konsument köper sina produkter.

Routrarna har efter inköpstillfället inte uppdaterats med eventuell ny firmware då vi inte tror att det är något som den normale hemanvändaren generellt gör. Detta beteende bekräftats av de tillverkare vi varit i kontakt med.

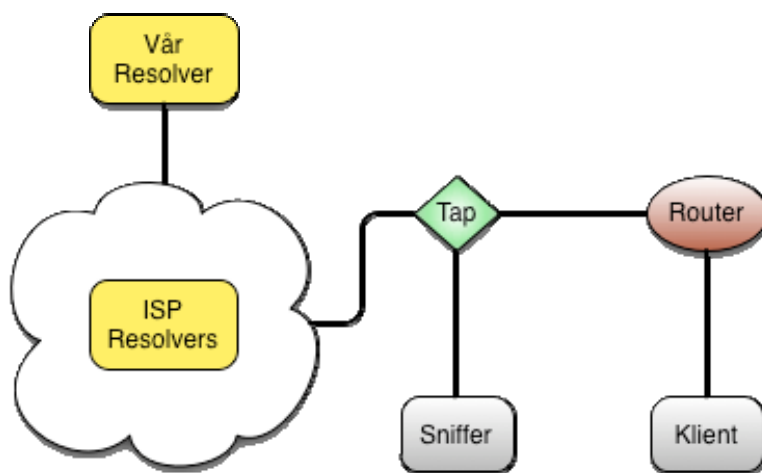
I testet används två datorer. En som sitter bakom routern och ställer testfrågorna och en som sitter mellan modemmet och routern och avlyssnar trafiken. Avlyssningsdatorn är inkopplad via en linjelyssnare som inte påverkar mätresultaten.

För att kunna genomföra testerna under realistiska förhållanden skaffade vi en Internetanslutning med ADSL från de båda Internetleverantörerna som vid tidpunkten hade DNSSEC-konfigurerade resolver. Testfrågorna ställs mot deras resolver, vilka under testerna körde BIND 9.4.2.

För de testfrågor som ska ställas till den version av BIND som innehåller buggen, har vi ändrat i routerinställningarna och ställt in den så att uppslagning sker till vår egna resolver. I övrigt har nätverksinställningarna ställts in med DHCP från leverantören.

2.4 Testmiljön

Vår testmiljö ser ut som på bilden nedan:



Figur 1: Testmiljö

Klient är en Apple Mac Mini med MacOS X version 10.5.1 och dig version 9.4.1-P1.

Router är den testade routern.

Mellan routern och Internet sitter en nätverkstapp av märket NetOptics, modell Teeny Tap.

Nätverkstappen är kopplad till ytterligare en Mac Mini med MacOS X 10.5.1, på den körs Wireshark (v.0.99.6) för att lyssna av trafiken mellan routern och "Internet".

Internetleverantörens resolver kör BIND 9.4.2 och vår resolver kör BIND 9.4.1.

2.5 Beskrivning av testerna

Testspecifikationen finns i bilaga 1.

Här följer en beskrivning av vad som testas i respektive fråga, alla tester är körda både i UDP och TCP:

A-frågorna testar stora paket i DNS. Gradvis större paket testade med olika stor bufferstorlek.

För att få godkänt måste all data levereras till klienten. Trunkering och timeout var två vanliga felaktiga svar.

Test *B.1* testar om routern tar emot paketet om AD-biten är satt, även då validering inte begärts av klienten. Det görs genom att ställa en fråga om en DNSSEC-signerad domän mot en vår resolver med BIND 9.4.1 (med AD-buggen). För godkänt krävs att paketet tas emot och att AD-biten är satt.

I test *B.2* ställs en likadan fråga som för *B.1* men mot Internetleverantörens AD-buggfria resolver. Denna gång saknar paketet AD-biten. Här krävs att paketet tas emot av routern och levererar det till klienten.

I test *C.1* ber klienten om ett validerat DNSSEC-svar från en domän som använder DNSSEC av ISP:ns resolver. I frågan sätts DO=1. (DO-flagga satt). Förväntat resultat för godkänt är ett svar med all DNSSEC-data från domänen, samt att svaret ska vara validerat med AD=1.

Test *C.2* ber klienten om DNSSEC-svar från en icke DNSSEC-signerad domän av ISP:ns resolver (DO-flagga satt). För godkänt krävs ett korrekt svar. Denna fråga ställs för att testa om routern klarar av att ta emot ett paket som den inte förväntar sig.

D.1 och *D.2* motsvarar *C.1* och *C.2* med tillägget att de även frågar efter CD=1 (resolvern ska inte genomföra DNSSEC-validering av svar). Här testas om routern även klarar CD-flaggan. För OK ska motsvarande svar som med C-frågorna visas, med skillnaden att AD inte är satt men att CD är det.

I test *E.1* frågas en DNSSEC-signerad domän via vår resolver med version 9.4.1 efter enbart AD=1. För godkänt krävs ett svar med AD=1.

E.2 gör samma sak som *E.1* men frågar via ISP:ns med version 9.4.2. Här förväntas ett resultat med AD=0.

F.1 är ett test om routern agerar som en öppen rekursiv resolver för datorer på routerns WAN-sida. Detta test körs från en dator som står "ute på internet". För godkänt skall den frågande datorn inte få något svar.

G.1 frågar efter IPv6 i DNS (AAAA).

G.2 testar SSH fingerprint i DNS (SSHFP).

G.3 frågar efter SRV-poster.

G.4 frågar efter NAPTR-poster.

G.5 testar om routern skickar vidare DNS-frågor om AS112-nät.

3 Resultatet i sammanfattning

3.1 Testresultatet

Av tolv testade routrar har tio genomgått testerna med blandat resultat. De två som vi inte lyckats testa har haft sådana problem att testresultaten inte gått att använda.

Av de tio testade routrarna har tre stycken passerat testprotokollet utan värre anmärkning. De återstående sju har haft märkbara problem vid mer avancerat användande av DNS.

De vanligaste felen har varit frågor och svar över TCP, problem med AD-biten i svaret samt när klienten vill validera DNSSEC själv (DO-biten satt i frågan).

Resultatet av testerna är nedslående. Vad som står ut mest är andelen routrar som inte klarar av DNS-frågor över TCP. Men det stora problemet ur DNSSEC-perspektiv är att majoriteten inte klarar av DNSSEC ner till applikationsnivå på datorn. Det är inget problem så länge valideringen sköts av t.ex. Internetleverantörens DNS-resolver, men när det tillkommer en applikation på klienten som begär egen DNSSEC-validering fungerar det i de flesta fall inte alls.

Att en router inte klarar av frågor över TCP innebär problem när DNS-paket är större än 512 bytes, i synnerhet då stödet för EDNS0 inte heller är särskilt bra.

Angående den sista testen, G.5 (AS112) så var det bara en router som filtrerade den typen av frågor.

3.2 Åtgärder

Vi har kontaktat tillverkarna av de produkter vi har testat. Några har återkommit med varierande grad av engagemang, och en har faktiskt tagit problemet på allvar och kommit med åtgärder.

3.3 Fortsatt arbete

De problem som finns hos konsumentroutrarna vad gäller DNS och DNSSEC gäller också i stort sett även IPv6, eftersom IP-paketerna väntas växa i storlek med tillväxten av dessa två tekniker. Att se till att dessa typer av produkter hanterar DNS korrekt är viktigt, då tillväxten annars hämmas. Internet består idag ändå av användare som använder den här typen av produkter. Nästa generations Internet bör klara av både DNSSEC och IPv6 både i nät och DNS med dess applikationer.

Vi vill att tillverkarna tar dessa problem på större allvar, och vi förutsätter att fler routrar ska testas. Ett internationellt samarbete bör startas med en gemensam uppsamlingsplats av resultaten.

4 Bilagor

4.1 Bilaga 1, DNS test protocol for SOHO-routers

Alla tester genomförs med både UDP och TCP i frågan.

*** Is the router capable of EDNS0

*** Does the router give the client ENDS0 traffic

A.1.1: dig +retry=0 +bufsize=512 +qr small.nxdomain.se TXT

A.1.2: dig +retry=0 +bufsize=512 +qr medium.nxdomain.se TXT

A.1.3: dig +retry=0 +bufsize=512 +qr large.nxdomain.se TXT

A.1.4: dig +retry=0 +bufsize=512 +qr huge.nxdomain.se TXT

A.2.1: dig +retry=0 +bufsize=1024 +qr small.nxdomain.se TXT

A.2.2: dig +retry=0 +bufsize=1024 +qr medium.nxdomain.se TXT

A.2.3: dig +retry=0 +bufsize=1024 +qr large.nxdomain.se TXT

A.2.4: dig +retry=0 +bufsize=1024 +qr huge.nxdomain.se TXT

A.3.1: dig +retry=0 +bufsize=4096 +qr small.nxdomain.se TXT

A.3.2: dig +retry=0 +bufsize=4096 +qr medium.nxdomain.se TXT

A.3.3: dig +retry=0 +bufsize=4096 +qr large.nxdomain.se TXT

A.3.4: dig +retry=0 +bufsize=4096 +qr huge.nxdomain.se TXT

A.4.1: dig +retry=0 +bufsize=8192 +qr small.nxdomain.se TXT

A.4.2: dig +retry=0 +bufsize=8192 +qr medium.nxdomain.se TXT

A.4.3: dig +retry=0 +bufsize=8192 +qr large.nxdomain.se TXT

A.4.4: dig +retry=0 +bufsize=8192 +qr huge.nxdomain.se TXT

**** AD=1 in the reply

*** Does the router accept replies with AD=1

B.1: dig +retry=0 @validator-with-BIND_9.4.1 +qr dnssec.se SOA

*** Does the router accept replies with AD=0

B.2: dig +retry=0 @validator-with-BIND_9.4.2 +qr dnssec.se SOA

*** DO=1 in query

*** Does the router accept queries with DO=1, replies with AD=1

C.1: dig +retry=0 @validator-with-BIND_9.4.2 +qr +dnssec dnssec.se SOA

*** Does the router accept queries with DO=1, replies with AD=0

C.2: dig +retry=0 @validator-with-BIND_9.4.2 +qr +dnssec iis.se SOA

*** DO=1, CD=1 in query

*** Does the router accept queries with DO=1, CD=1

D.1: dig +retry=0 @validator-with-BIND_9.4.2 +qr +dnssec +cdflag dnssec.se SOA

*** Does the router accept queries with DO=1, CD=1

D.2: dig +retry=0 @validator-with-BIND_9.4.2 +qr +dnssec +cdflag iis.se SOA

*** AD=1 in query

*** Does the router accept queries with AD=1, replies with AD=1

E.1: dig +retry=0 @validator-with-BIND_9.4.1 +qr +adflag dnssec.se SOA

*** Does the router accept queries with AD=1, replies with AD=0

E.2: dig +retry=0 @validator-with-BIND_9.4.2 +qr +adflag dnssec.se SOA

*** Open resolver in the router? (test from the "WAN side")

F.1: dig +retry=0 @router nonexistent.dnssec.se TXT

*** Misc RR types

*** Does the router let miscellaneous RR types through

G.1: dig +retry=0 boa.blipp.com AAAA

G.2: dig +retry=0 boa.blipp.com SSHFP

G.3: dig +retry=0 _sip_tcp.blipp.com SRV

G.4: dig +retry=0 blipp.com NAPTR

*** Does the router forward AS112 in-addr.arpa queries

G.5 dig +retry=0 1.0.168.192.in-addr.arpa. PTR

4.2 Bilaga 2, Resultat från testprotokoll

Router:	D-Link DIR-100		D-Link DI-804HV		D-Link DI-624+		Netgear RP614	
Firmware:	v1.00		V1.44		V1.23		V0.1.8_03.17	
Test:	UDP	TCP	UDP	TCP	UDP	TCP	UDP	TCP
A.1.1	OK	FAILED	OK	OK	OK	FAILED	OK	FAILED
A.1.2	FAILED	FAILED	OK	OK	FAILED	FAILED	FAILED	FAILED
A.1.3	FAILED	FAILED	OK	OK	FAILED	FAILED	FAILED	FAILED
A.1.4	FAILED	FAILED	OK	OK	FAILED	FAILED	FAILED	FAILED
A.2.1	OK	FAILED	OK	OK	OK	FAILED	OK	FAILED
A.2.2	FAILED	FAILED	OK	OK	FAILED	FAILED	FAILED	FAILED
A.2.3	FAILED	FAILED	OK	OK	FAILED	FAILED	FAILED	FAILED
A.2.4	FAILED	FAILED	OK	OK	FAILED	FAILED	FAILED	FAILED
A.3.1	OK	FAILED	OK	OK	OK	FAILED	OK	FAILED
A.3.2	FAILED	FAILED	OK	OK	OK	FAILED	FAILED	FAILED
A.3.3	FAILED	FAILED	OK	OK	FAILED	FAILED	FAILED	FAILED
A.3.4	FAILED	FAILED	OK	OK	FAILED	FAILED	FAILED	FAILED
A.4.1	OK	FAILED	OK	OK	OK	FAILED	OK	FAILED
A.4.2	FAILED	FAILED	OK	OK	OK	FAILED	FAILED	FAILED
A.4.3	FAILED	FAILED	OK	OK	FAILED	FAILED	FAILED	FAILED
A.4.4	FAILED	FAILED	OK	OK	FAILED	FAILED	FAILED	FAILED
B.1	FAILED	FAILED	OK	OK	OK	FAILED	FAILED	FAILED
B.2	OK	FAILED	OK	OK	OK	FAILED	OK	FAILED
C.1	FAILED	FAILED	OK	OK	FAILED	FAILED	OK	FAILED
C.2	OK	FAILED	OK	OK	OK	FAILED	OK	FAILED
D.1	FAILED	FAILED	OK	OK	FAILED	FAILED	FAILED	FAILED
D.2	FAILED	FAILED	OK	OK	OK	FAILED	FAILED	FAILED
E.1	FAILED	FAILED	OK	OK	OK	FAILED	FAILED	FAILED
E.2	FAILED	FAILED	OK	OK	OK	FAILED	FAILED	FAILED
F.1	FAILED	FAILED	OK	OK	OK	OK	FAILED	FAILED
G.1	OK	FAILED	OK	OK	OK	FAILED	OK	FAILED
G.2	OK	FAILED	OK	OK	OK	FAILED	OK	FAILED
G.3	OK	FAILED	OK	OK	OK	FAILED	OK	FAILED
G.4	OK	FAILED	OK	OK	OK	FAILED	OK	FAILED
G.5	FAILED	FAILED	FAILED	FAILED	FAILED	FAILED	FAILED	FAILED

Router:	Netgear WNR834B		Netgear WGR614		Netgear WPN824		Linksys WRT54GS	
Firmware:	V1.0.4.0WW		V2.0.20_1.0.20		V2.0.10_1.2.17		v1.50.6	
Test:	UDP	TCP	UDP	TCP	UDP	TCP	UDP	TCP
A.1.1	OK	FAILED	OK	FAILED	OK	FAILED	OK	OK
A.1.2	FAILED	FAILED	FAILED	FAILED	FAILED	FAILED	OK	OK
A.1.3	FAILED	FAILED	FAILED	FAILED	FAILED	FAILED	OK	OK
A.1.4	FAILED	FAILED	FAILED	FAILED	FAILED	FAILED	OK	OK
A.2.1	OK	FAILED	OK	FAILED	OK	FAILED	OK	OK
A.2.2	FAILED	FAILED	FAILED	FAILED	FAILED	FAILED	OK	OK
A.2.3	FAILED	FAILED	FAILED	FAILED	FAILED	FAILED	OK	OK
A.2.4	FAILED	FAILED	FAILED	FAILED	FAILED	FAILED	OK	OK
A.3.1	OK	FAILED	OK	FAILED	OK	FAILED	OK	OK
A.3.2	FAILED	FAILED	OK	FAILED	OK	FAILED	OK	OK
A.3.3	FAILED	FAILED	FAILED	FAILED	FAILED	FAILED	OK	OK
A.3.4	FAILED	FAILED	FAILED	FAILED	FAILED	FAILED	OK	OK
A.4.1	OK	FAILED	OK	FAILED	OK	FAILED	OK	OK
A.4.2	FAILED	FAILED	OK	FAILED	OK	FAILED	OK	OK
A.4.3	FAILED	FAILED	OK	FAILED	FAILED	FAILED	OK	OK
A.4.4	FAILED	FAILED	FAILED	FAILED	FAILED	FAILED	OK	OK
B.1	FAILED	FAILED	OK	FAILED	Untested	Untested	OK	OK
B.2	FAILED	FAILED	OK	FAILED	OK	FAILED	OK	OK
C.1	FAILED	FAILED	OK	FAILED	OK	FAILED	OK	OK
C.2	OK	FAILED	OK	FAILED	OK	FAILED	OK	OK
D.1	FAILED	FAILED	OK	FAILED	OK	FAILED	OK	OK
D.2	FAILED	FAILED	OK	FAILED	OK	FAILED	OK	OK
E.1	FAILED	FAILED	OK	FAILED	Untested	Untested	OK	OK
E.2	FAILED	FAILED	OK	FAILED	OK	FAILED	OK	OK
F.1	OK	OK	OK	OK	OK	OK	OK	OK
G.1	OK	FAILED	OK	FAILED	OK	FAILED	OK	OK
G.2	OK	FAILED	OK	FAILED	OK	FAILED	OK	OK
G.3	OK	FAILED	OK	FAILED	OK	FAILED	OK	OK
G.4	OK	FAILED	OK	FAILED	OK	FAILED	OK	OK
G.5	FAILED	FAILED	FAILED	FAILED	FAILED	FAILED	FAILED	FAILED

Router:		Zyxel P-320W	FON	
Firmware:		V1.00(ZH.3)C0	0.7.2 r2	
Test:	UDP	TCP	UDP	TCP
A.1.1	OK	FAILED	OK	OK
A.1.2	FAILED	FAILED	OK	OK
A.1.3	FAILED	FAILED	OK	OK
A.1.4	FAILED	FAILED	OK	OK
A.2.1	OK	FAILED	OK	OK
A.2.2	FAILED	FAILED	OK	OK
A.2.3	FAILED	FAILED	OK	OK
A.2.4	FAILED	FAILED	OK	OK
A.3.1	OK	FAILED	OK	OK
A.3.2	FAILED	FAILED	OK	OK
A.3.3	FAILED	FAILED	OK	OK
A.3.4	FAILED	FAILED	OK	OK
A.4.1	OK	FAILED	OK	OK
A.4.2	FAILED	FAILED	OK	OK
A.4.3	FAILED	FAILED	OK	OK
A.4.4	FAILED	FAILED	OK	OK
B.1	OK	FAILED	Untested	Untested
B.2	OK	FAILED	OK	OK
C.1	FAILED	FAILED	OK	OK
C.2	OK	FAILED	OK	OK
D.1	FAILED	FAILED	OK	OK
D.2	FAILED	FAILED	OK	OK
E.1	OK	FAILED	Untested	Untested
E.2	OK	FAILED	OK	OK
F.1	OK	OK	OK	OK
G.1	OK	FAILED	OK	OK
G.2	OK	FAILED	OK	OK
G.3	OK	FAILED	OK	OK
G.4	OK	FAILED	OK	OK
G.5	FAILED	FAILED	OK	OK