Primerjava strežnikov s podporo DNSSEC

Dušan Kozic, Luka Koršič[1], Janez Sterle[1], Andrej Kos[1]

[1]*Univerza v Ljubljani, Fakulteta za elektrotehniko, Laboratorij za telekomunikacije*
E-pošta: dusan.kozic@ltfe.org

Comparison of DNSSEC enabled DNS servers

It is known for a while, that DNS by itself does not have sufficient security mechanisms implemented. For this purpose, a security extension of the DNS protocol is being standardized and developed, called DNSSEC. It provides authentication and integrity to DNS messages, however it doesn't provide confidentiality. DNSSEC relies on the public key cryptography.

In this article we wanted to explore implementations of DNSSEC server software that is available at the moment. We set up a DNSSEC environment, where we set up most widely used authoritative and recursive DNS servers, and a few domains in which we tested DNSSEC. The results showed that server solutions are currently in mature phase of development. Two of the three authoritative server solutions and two of the three recursive server solutions support all of the DNSSEC standards. The remaining solution is still missing some features from the latest DNSSEC standards and will most likely be updated in the (near) future.

1 Uvod

Internet brez protokola DNS (angl. Domain Name System) ne bi bil internet, kakršnega si predstavljamo danes. DNS nam omogoča, da lahko namesto naslovov IP uporabljamo nam prijazna imena. Protokol DNS je ključen tudi za delovanje elektronske pošte.

Ob pisanju protokola DNS se ni veliko razmišljalo o varnosti. Vsa sporočila DNS se pošiljajo v nešifrirani obliki, zato lahko napadalec, ki se vrine med nas in strežnik DNS ali med dva strežnika DNS, vidi, po katerih naslovih sprašujemo, poleg tega pa lahko ta sporočila tudi po želji spreminja. Tako nas lahko namerno zavede na napačen strežnik. Protokol DNS je ranljiv tudi na napade v primeru, ko napadalec ne prisluškuje komunikaciji. Leta 2008 je Dan Kaminsky z enim takšnih napadov (napad aktivnega zastrupljanja medpomnilnika DNS) dokončno dokazal, da je v sistem DNS potrebno vgraditi dodatne varnostne mehanizme. [1]

Odgovor strokovnjakov za računalniško varnost je bil, da se naj varnostna razširitev protokola DNS, imenovana DNSSEC (angl. Domain Name System Security Extensions), ki se razvija že od leta 1995, začne postopoma uvajati v internetno uporabo.

V članku bodo na kratko predstavljene osnove DNSSEC ter vzpostavitev testnega okolja DNSSEC na avtoritativnih in rekurzivnih strežnikih z namenom primerjave rešitev DNSSEC na različnih strežniških sistemih.

2 DNSSEC

DNSSEC je varnostna razširitev protokola DNS. Protokolu DNS dodaja mehanizme za zagotavljanje avtentikacije in integritete ter tako uspešno rešuje problem podtikanja ponarejenih odgovorov DNS, kar predstavlja glavni varnostni problem protokola DNS. DNSSEC nam zaupnosti pri poizvedovanju ne nudi. Definiran je v standardih RFC 4033-4035 (iz leta 2005) [2][3][4] ter naknadno dopolnjen s standardi RFC 4509 (2006) [5], RFC 5011 (2007) [6], 5155 (2008) [7], 5702 (2009) [8]. Kot varnostni mehanizem uporablja digitalni podpis, ki vključuje uporabo kriptografije z javnim ključem in zgoščevalnih funkcij. Za digitalno podpisovanje uporablja algoritme DSA/SHA-1, RSA/SHA-1 ter RSA/SHA-256 in RSA/SHA-512 (uporaba algoritmov RSA/SHA-256 in RSA/SHA-512 je predvidena naknadno v RFC 5702 iz leta 2009).

2.1 Zapisi DNSSEC

DNSSEC sistemu DNS prinaša 5 novih zapisov. To so DNSKEY, RRSIG, DS, NSEC, NSEC3 in NSEC3PARAM. NSEC3 in NSEC3PARAM sta novejša zapisa uvedena naknadno v RFC 5155.

Zapis DNSKEY predstavlja zapis javnega ključa, s katerim lahko preverimo podpise RRSIG vseh ostalih zapisov DNS v zoni. Obstajata dva tipa ključev DNSKEY: KSK (angl. Key Signing Key) in ZSK (angl. Zone Signing Key). Z ZSK so podpisani vsi zapisi v zoni, s KSK pa je podpisan ZSK. Ključe moramo na določeno časovno obdobje tudi zamenjati, saj se z daljšim časom uporabe ključev veča tudi možnost, da bo nekdo naš ključ razbil. Dva ključa uporabljamo z razlogom, ker želimo ključ KSK menjavati manj pogosto, saj moramo izvleček ključa KSK v obliki zapisa DS ob menjavi sporočiti starševski zoni, ki je na ločenem strežniku in tipično ni v našem upravljanju. Priporočen čas menjave ključa ZSK je enkrat na 4 mesece, ključa KSK pa enkrat na leto. Ključ ZSK bi naj bil dolg najmanj 1024 bitov, ključ KSK pa 2048 bitov. [9]

Zapis RRSIG predstavlja digitalni podpis posameznega RRSET. RRSET predstavlja vse zapise DNS, ki imajo enako ime in so istega tipa. Z RRSIG so podpisani tudi vsi ostali zapisi, ki jih prinaša DNSSEC.

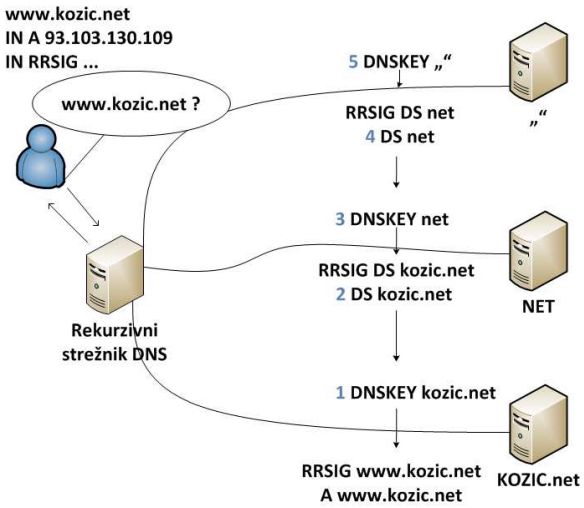
Podpisati je potrebno tudi negativne odgovore. V primeru, da negativnih odgovorov ne bi podpisovali, bi

lahko napadalec vrnil nelegitimen odgovor, s katerim bi sporočil da iskana domena ne obstaja ter tako naredil domeno nedostopno. Pri DNSSEC se zona najprej podpiše in šele nato naloži v strežnik. Strežnik praviloma pri sebi nima privatnega ključa, s katerim je zona podpisana, zato negativnih odgovorov ne more podpisovati v realnem času. Za negativne odgovore so tako uvedli zapis NSEC, ki nam pove, med katerimi zapisi v zoni ni obstoječih zapisov. Če sprašujemo po neobstoječem zapisu b.kozic.net, bo strežnik vrnil odgovor a.kozic.net IN NSEC c.kozic.net, s čimer pove, da med a.kozic.net in c.kozic.net zapis ne obstaja. S tem pa napadalcu še posredno izda, da v zoni obstajata tudi zapisa a.kozic.net in c.kozic.net. To mu omogoča, da se s povpraševanjem po zapisih NSEC dokoplje do celotne vsebine zone, česar pa si administrator ne želi. Kot rešitev pomanjkljivosti zapisa NSEC je bil naknadno uveden zapis NSEC3 (RFC 5155 iz leta 2008), ki namesto z originalnimi imeni odgovarja z njihovimi izvlečki. Zapis NSEC3PARAM uporabljajo izključno avtoritativni strežniki DNS pri kreiranju odgovorov NSEC3.

2.2 Veriga zaupanja

Pri DNSSEC je potrebno nujno ločiti vlogi avtoritativnega in rekurzivnega strežnika, saj avtoritativni strežnik ne more digitalno preverjati domen, za katere je avtoritativen.

Digitalno preverjanje zapisov DNSSEC, ki se izvaja na rekurzivnih strežnikih DNS, poteka ravno obratno kot poizvedovanje. Po drevesu DNS poizvedujemo od korenske domene navzdol, zapise DNSSEC pa digitalno preverjamo od imena iskane domene navzgor. Digitalno preverjanje zapisa A www.kozic.net bi tako potekalo po sledečem postopku prikazanem na sliki 1:



Slika 1: Primer digitalnega preverjanja domene www.kozic.net

1) najprej preverimo podpis RRSIG zapisa A www.kozic.net, ki je podpisan s ključem DNSKEY domene kozic.net,
2) za zapis DNSKEY kozic.net obstaja v starševski domeni .net zapis DS,
3) podpis RRSIG zapisa DS kozic.net je podpisan s ključem DNSKEY domene .net,
4) za zapis DNSKEY .net obstaja v starševski korenski domeni zapis DS,
5) podpis RRSIG tega zapisa je podpisan s ključem DNSKEY korenske domene.

Ključu korenske domene moramo zaupati. Na varen način ga lahko prenesemo s spletne strani IANA. Če bo digitalno preverjanje domene uspešno bo strežnik DNS odgovoru dodal zastavico AD (angl. Authenticated Data). [10]

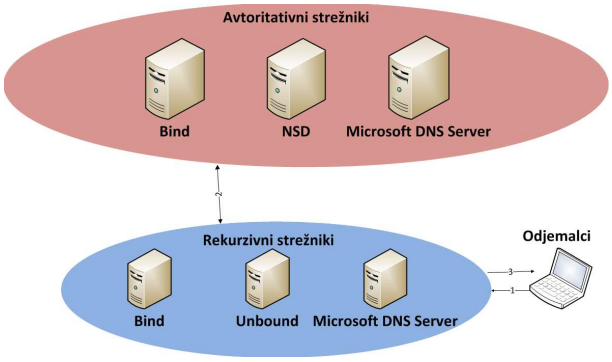
Digitalno preverjanje domen je možno od trenutka, ko je korenska domena podpisana. Obstajajo tudi alternativne možnosti digitalnega preverjanja domen. Ena izmed njih je projekt ISC DLV, ki ima zgrajeno svojo verigo zaupanja. Poleg tega je možno zgraditi t.i. sidra zaupanja med različnimi strežniki DNS, kar v praksi pomeni, da ima lahko npr. posamična organizacija svoj rekurzivni strežnik DNS, ki digitalno preverja njihove domene, medtem ko v starševski domeni nima vnesenih zapisov DS svojih domen.

3 Postavitev okolja DNSSEC

S postavitvijo testnega okolja DNSSEC smo želeli v praksi preveriti, kakšno je trenutno stanje podprtosti DNSSEC na strežnikih. Zanimala nas je kompleksnost njihove konfiguracije in vzdrževanja ter podprtost različnih standardov RFC. V ta namen smo postavili 3 avtoritativne in 3 rekurzivne strežnike. Kot avtoritativne strežnike smo uporabili Bind [11], NSD [12] in Microsoft DNS Server [13], kot rekurzivne pa Bind, Unbound [14] in Microsoft DNS Server. Za testiranje smo uporabili zone sah-drustvo-ms.si, kozic.net in ltfe-sphere.org. Zonam smo dodatno naredili poddomene, ki smo jih ustrezno delegirali med različne avtoritativne strežnike DNS. Najbolj zapleteno delo na avtoritativnih strežnikih je bilo ponovno podpisovanje zon in vzdrževanje ključev. Slednje ne more biti popolnoma avtomatizirano, saj je potrebno spremembe ključa DNSKEY v obliki zapisa DS posredovati starševski zoni, ki je običajno na drugem strežniku DNS in ni pod enotnim upravljanjem.

Rekurzivne strežnike smo uporabili za digitalno preverjanje naših testnih zon. Nekatere podpise in zapis DS ene izmed zon smo namerno pokvarili. Tako smo želeli preizkusiti, ali bo rekurzivni strežnik ustrezno zaznal nepravilne zapise DNS ter kako bo v takem primeru reagiral.

Postavitev testnega okolja je prikazana na sliki 2 in v tabelah 1 in 2.



Slika 2: Topologija testnega okolja

Tabela 1: Domene na avtoritativnih strežnikih DNS

Avtoritativni strežnik	Zona	Vrsta zaupanja	Delegirana domena
Bind	kozic.net	DLV	bind.ltfe-sphere.org
NSD	sah-drustvo-ms.si	Sidro zaupanja	nsd.kozic.net
Microsoft DNS	ltfe-sphere.org	DS	ms.sah-drustvo-ms.si

Tabela 2: Algoritmi za digitalno podpisovanje po zonah

Zona	Algoritem	Negativni odgovor
kozic.net	RSA/SHA-1	NSEC3
sah-drustvo-ms.si	RSA/SHA-256	NSEC3
ltfe-sphere.org	RSA/SHA-1	NSEC
nsd.kozic.net	RSA/SHA-256	NSEC3
ms.sah-drustvo-ms.si	RSA/SHA-1	NSEC
bind.ltfe-sphere.org	RSA/SHA-1	NSEC3

4 Primerjava strežnikov DNS

4.1 Avtoritativni strežniki

Na avtoritativnih strežnikih smo se odločili primerjati:
- podporo standardom DNSSEC,
- način nastavitve DNSSEC,
- podporo dinamičnemu zagotavljanju DNSSEC ter
- možnost samodejnega vzdrževanja podpisane zone.

Bind ima polno podporo vsem standardov DNSSEC. Nastavitev poteka v ukazni lupini in ni zapletena. DNSSEC smo vklopili z enim stavkom, za podpisovanje zon pa ima Bind vgrajena orodja. Možna je uporaba dinamičnega DNSSEC, pri tem pa je potrebno opomniti, da je v tem primeru strežniku DNS na voljo privatni ključ, kar pomeni, da se napadalec lahko v primeru, da obstaja varnostna luknja v strežniku, dokoplje do našega privatnega ključa. To je cena, ki jo zahteva uporaba dinamičnega DNSSEC in velja za vse rešitve DNSSEC. Bind je prav tako zmožen samodejno vzdrževati podpisano zono, saj podpise pred potekom samodejno obnovi. Ključe smo samodejno menjali tako, da smo starim ključem določili, kdaj prenehajo veljati in novim, kdaj začnejo veljati. To pomeni, da menjava ni povsem avtomatična, saj smo morali pred menjavo ključev, le-te ročno kreirati. Čase, kdaj naj Bind umakne stare ključe iz zone in kdaj jo naj podpiše z novimi, smo morali pozorno definirati. Če bi pri teh časih zgrešili, bi imeli zono nekaj časa nepravilno podpisano.

Microsoft DNS Server ima podporo zgolj osnovnim standardom DNSSEC (RFC 4033-4035), zato je glede podpisovanja zon omejen na algoritem RSA/SHA-1. Problematična pa je zlasti uporaba NSEC za negativne odgovore. Tako je vsebina naših zon, ki jih je serviral Microsoft DNS Server, bila javna. Strežnik ima omogočen pregled DNSSEC podpisanih zon preko grafičnega vmesnika, žal pa nam ni omogočal grafičnega upravljanja DNSSEC. Nastavitev DNSSEC mora potekati v ukazni vrstici, Microsoft pa je objavil tudi skripte PowerShell, ki so nam tako nastavitev olajšale. Dinamičen DNSSEC v Microsoft DNS Server ni podprt. Menjavo ključev in ponovno podpisovanje zon smo morali izvajati ročno, skripta PowerShell pa nam je preko uporabniškega vmesnika menjavo ključev olajšala, saj je delovala interaktivno in nam sproti tudi dajala navodila, kaj moramo storiti. Tako je bila tudi možnost napak manjša.

NSD ima tako kot Bind, polno podporo vsem standardom DNSSEC. DNSSEC nam na strežniku DNS ni bilo treba posebej vklopiti, vse kar smo morali narediti je, da smo strežniku podali podpisano datoteko zone. NSD nam ne prinaša nobenih orodij za podpisovanje zon in generiranje ključev, so pa ta orodja del paketa ldns, ki ga je izdala ista organizacija kot strežnik NSD. NSD je lahko serviral tudi zone, ki so bile podpisane z orodji strežnika Bind ali Microsoft DNS. Dinamičnega DNSSEC pri NSD prav tako nismo mogli uporabljati. Ker NSD ne vsebuje orodij za podpisovanje zon in generiranje ključev, samodejno vzdrževanje zone na tem strežniku ni bilo možno.

Tabela 3: Primerjava avtoritativnih strežnikov DNS

	Microsoft DNS Server	Bind	NSD
Podprti algoritmi	samo RSA/SHA-1	vsi	vsi
Negativni odgovori	NSEC	NSEC, NSEC3	NSEC, NSEC3
Preprostost konfiguracije	srednja	srednja	srednja
Dinamičen DNSSEC	ne	da	ne
Samodejno vzdrževanje zone	ne	deloma	ne

4.2 Rekurzivni strežniki

Na rekurzivnih strežnikih smo digitalno preverjali naše testne domene. Odločili smo se primerjati:
- podporo standardom DNSSEC,
- različne verige zaupanja pri digitalnem preverjanju domen,
- obnašanje v primeru napak,
- preprostost nastavitev.

Bind tudi pri digitalnem preverjanju domen podpira vse standarde DNSSEC. Zmožen je preverjati vse tri verige zaupanja. V primeru napake ob digitalnem preverjanju domen ne vrne zastavice AD, prav tako pa

ne vrne neveljavnega odgovora DNS. Neveljavnega odgovora ne vrne tudi odjemalcu, ki ni sprožil DNSSEC poizvedbe, vrne pa mu napako SERVFAIL. Bind poleg vklopa DNSSEC dodatno zahteva še vklop digitalnega preverjanja domen in potrebno mu je tudi povedati, katero drevo naj preverja (celotno drevo, ISC DLV). Ključev nam ni treba uvažati, saj so nam že na voljo, prav tako bo Bind samodejno zamenjal ključe KSK, ko se bodo le-ti spremenili.

Microsoft DNS Server podpira zgolj osnovne standarde RFC, zato ne more digitalno preverjati korenske domene, ki je podpisana z algoritmom RSA/SHA-256, prav tako pa ne velike večine vrhnjih domen TLD (angl. Top Level Domain), saj le-te uporabljajo NSEC3 za negativne odgovore. Za digitano preverjanje torej ni primeren. V primeru sidra zaupanja vnesenega za domeno ltfe-sphere.org, je digitalno preverjanje domene delovalo. Microsoft DNS prav tako ne podpira uporabe alternativnega drevesa DNSSEC ISC DLV. V primeru napak ob digitalnem preverjanju domen se obnaša tako kot Bind, konfiguracija Microsoft DNS kot rekurzivnega strežnika DNS pa je možna tudi v grafičnem načinu.

Unbound podpira vse standarde DNSSEC in je bil zmožen digitalno preverjati vse tri verige zaupanja. V primeru napak ob digitalnem preverjanju domen, se je obnašal enako kot ostala dva strežnika. Digitalnega preverjanja domen v strežniku Unbound ni potrebno posebej vklopiti, mu je pa potrebno podati pot do datotek s ključi domen, ki jih želimo preverjati. Unbound sicer nima pred naloženega ključa KSK korenske domene, vsebuje pa digitalno potrdilo strežnika IANA, s katerega smo lahko z enim ukazom na varen način prenesli zapis DS ključa korenske domene. V strežnik Unbound nam kot sidro zaupanja ni bilo potrebno vnesti ključa KSK, lahko smo vnesli tudi zapis DS tega ključa. Unbound prav tako podpira samodejno posodabljanje ključa KSK oz. njegovega zapisa DS, ne podpira pa samodejnega posodabljanja ključa KSK alternativnega drevesa ISC DLV.

Tabela 4: Primerjava rekurzivnih strežnikov DNS

	Microsoft DNS Server	**Bind**	**Unbound**
Podprti algoritmi	RSA/SHA-1 NSEC	vsi	vsi
Podprte verige zaupanja	sidra zaupanja	vse	vse
Obnašanje v primeru napake	pravilno	pravilno	pravilno
Preprostost nastavitev	velika (grafični vmesnik)	velika	velika

5 Sklep

V prispevku smo naredili primerjavo podpore DNSSEC med različnimi strežniki DNS. Izkaže se, da je za uporabo DNSSEC med avtoritativnimi strežniki trenutno najboljši Bind, ki poleg tega, da podpira uporabo dinamičnega DNSSEC, deloma podpira tudi samodejno vzdrževanje zon. Tako administratorjem olajša delo in zmanjšuje možnost napak. Med rekurzivnimi strežniki sta strežnika Bind in Unbound enakovredna. Glavna pomanjkljivost Microsoft DNS Server je, da le-ta še nima podpore novejšim standardom RFC. Poleg tega bo za lažje upravljanje najverjetneje Microsoft moral nadgraditi grafični vmesnik za delo z DNSSEC v njihovem okolju.

DNSSEC je s strani strežnikov v trenutni fazi zadostno implementiran, bo pa potrebnega še veliko dela na aplikacijah in sistemih za odjemalce, kar sicer ni bil predmet tega članka. Zagotoviti bo potrebno tudi učinkovit sistem za generiranje ključev in vzdrževanje zon ter premisliti ali je za to delo sploh še smotrno uporabljati strežnike DNS ali pa se naj to delo prepusti specializirani programski opremi.

Pri DNSSEC se vedno poraja vprašanje v kolikšni meri in če sploh bo zaživel. Ne gre toliko za vprašanje infrastrukture korenskih in vrhnjih strežnikov, saj ga bodo kmalu vsi podpirali, ampak bolj za vprašanje uporabnikov in organizacij, ali se jim to splača. DNS sicer ni varen, očitno pa še vedno zadovoljuje potrebe za katere je namenjen.

Literatura

[1] An Illustrated Guide to the Kaminsky DNS Vulnerability, http://www.unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html, dostopno julija 2011.

[2] RFC 4033, http://www.rfc-archive.org/getrfc.php?rfc=4033, dostopno julija 2011.

[3] RFC 4034, http://www.rfc-archive.org/getrfc.php?rfc=4034, dostopno julija 2011.

[4] RFC 4035, http://www.rfc-archive.org/getrfc.php?rfc=4035, dostopno julija 2011.

[5] RFC 4509, http://www.rfc-archive.org/getrfc.php?rfc=4509, dostopno julija 2011.

[6] RFC 5011, http://www.rfc-archive.org/getrfc.php?rfc=5011, dostopno julija 2011.

[7] RFC 5155, http://www.rfc-archive.org/getrfc.php?rfc=5155, dostopno julija 2011.

[8] RFC 5702, http://www.rfc-archive.org/getrfc.php?rfc=5702, dostopno julija 2011.

[9] RFC 4641, http://rfc-ref.org/RFC-TEXTS/4641/, dostopno julija 2011.

[10] P. Albitz, C. Liu, *DNS and Bind*, Sebastopol: O'Reilly Media, 2006, pogl. 11.

[11] Bind Documentation, http://www.isc.org/software/bind/documentation, dostopno julija 2011.

[12] NSD Documentation, http://nlnetlabs.nl/projects/nsd/documentation.html, dostopno julija 2011.

[13] Microsoft, DNSSEC Deployment Guide, http://www.microsoft.com/downloads/en/details.aspx?FamilyID=7a005a14-f740-4689-8c43-9952b5c3d36f&displaylang=en, dostopno julija 2011.

[14] Unbound Documentation, http://unbound.net/documentation, dostopno julija 2011.