pika na si
bilten registra za vrhnjo domeno .si

register.si
št. 1/2011

DNSSEC
Večja varnost na internetu

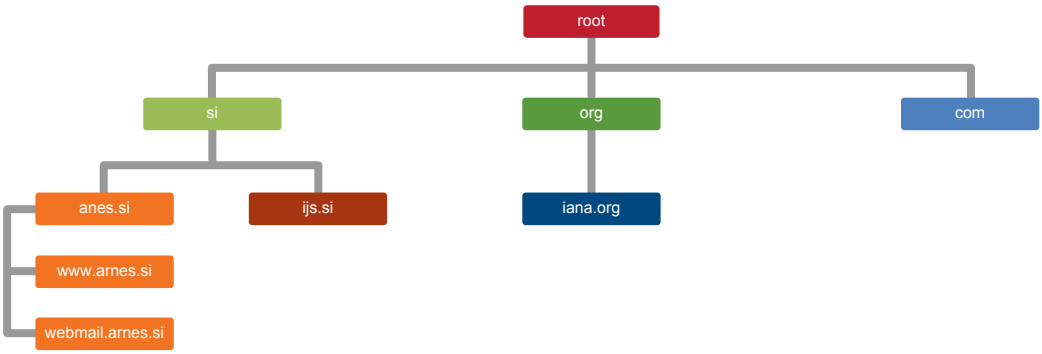
Kaj je DNSSEC?

DNSSEC je razširitev DNS-a, ki je ustvarjena z namenom, da zagotavlja avtentičnost in celovitost podatkov.

Računalnik, ki poizveduje po določenem IP-naslovu, lahko z DNSSEC tehnologijo preveri, če je DNS odgovor bil spremenjen med potovanjem po omrežju.

DNSSEC zagotavlja, da je obiskovalec dejansko na spletni strani na katero je imel namen priti. To jamstvo je ustvarjeno s pomočjo kriptografskih podpisov. DNS odgovori so podpisani tako da je moč preveriti ali gre za avtentične odgovore ali ne. Zapisi v DNSSEC-u niso šifrirani, vsi podatki so javno dostopni kot v obstoječem DNS-u.

Spletni brskalniki imajo že sedaj način overjanja spletnih strani oz. zagotavljajo, da je obiskovalec na “pravem mestu”. Take spletne strani so šifrirane s SSL tehnologijo. DNSSEC ni bil razvit z namenom, da zamenja SSL tehnologijo, temveč kot dodatno zavarovanje v primeru, da obiskovalec pristane na napačnem strežniku še preden je bila vzpostavljena varna povezava prek SSL.



Slika 1: DNS je hierarhičen sistem, kjer strežniki za .si posredujejo zahtevke po .si domenah (npr. www.arnes.si) na pravi IP-naslov.

Kako deluje DNS?

Internet temelji na hierarhičnem domenskem sistemu, s kratico imenovanem, DNS (Domain Name System). DNS preslika domene (kot je www.arnes.si) v IP-naslov (193.2.1.87). Domene uporabljamo zato, ker si jih lažje zapomnimo kot IP-številke. Zaradi porazdelitve bremena je DNS razdeljen na t.i. domene oz. cone. Na vrhu hierarhije je korenski strežnik (root), po hierarhiji mu sledijo strežniki za vrhnje domene in nato strežniki za domene (npr. arnes.si). Vsaka raven, ki ne pozna odgovora, bo poslala vprašanje na naslednjo nižjo raven. Če iščemo www.arnes.si bo root strežnik zahtevek posredoval na strežnik, ki je odgovoren za .si, le-ta pa bo zahtevek usmeril na strežnik, ki je odgovoren

za arnes.si. Strežnik odgovoren za arnes.si pa bo odgovoril katera je IP-številka, kjer se nahaja spletna stran (www) domene arnes.si.

Zakaj potrebujemo DNSSEC?

Predstavljajte si, da lahko nekdo drug kakor Telekom Slovenije spremeni telefonsko številko v telefonskem imeniku Slovenije. Uporabnik telefonskega imenika ne bi bil zmožen odkriti prevare.

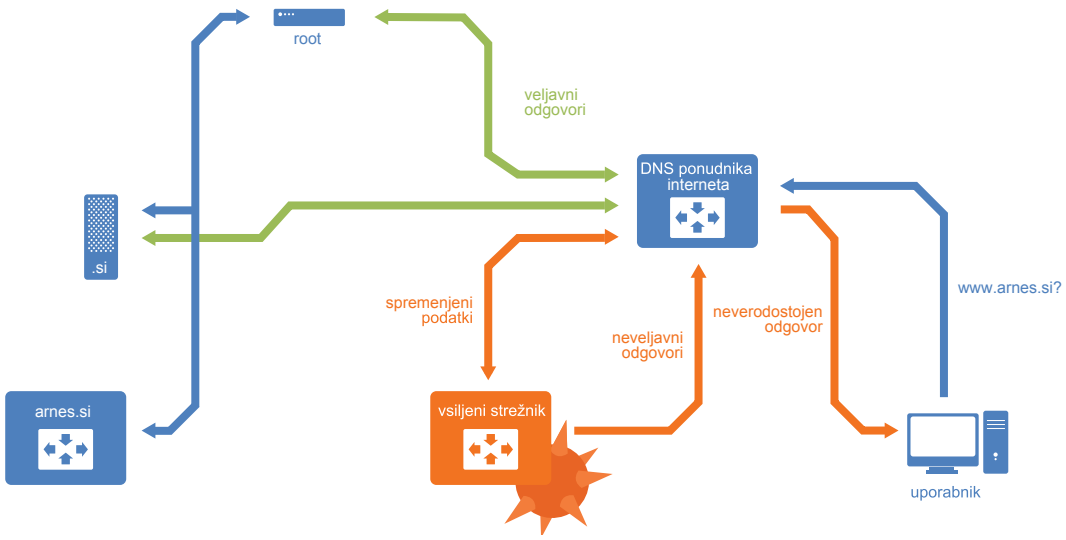
Nekaj podobnega se zgodi, če napadalec uspešno vstavi lažne podatke v DNS strežnik (cache poisoning). Namesto prave IP-številke strani www.arnes.si, bi prejeli drug IP. Škoda bi bila precejšnja, če bi se to zgodilo pri dostopu do spletnega bančništva ali pri pošiljanju zaupnih dokumentov, ki bi romali na lažni poštni strežnik.

Ker internet uporabljamo za mnoga opravila, imajo lahko takšne ranljivosti DNS-a velike posledice. DNSSEC predstavlja rešitev pred man-in-the-middle oz. cache poisoning napadi, ne zaščiti nas pa npr. pred phishing napadi. Phishing napade je možno preprečiti, tako da se obvesti in opozori uporabnike. DNS napade pa je zelo težko opaziti.

DNSSEC podpiše trenutne DNS zapise in nam s temi podpisi omogoči preverjanje avtentičnosti zapisov v DNS.

Vsi podatki določene domene so podpisani z zasebnim ključem, podpisi pa so vpisani v DNS kot RRSIG zapisi.

Rekurzivni strežnik bo po navadni poti v DNS hierarhiji poizvedel po IP-naslovu strani, hkrati pa bo na podlagi podpisov lahko preveril ali so odgovori DNS-a avtentični ali pa so bili spremenjeni.



Slika 2: DNSSEC zagotavlja, da je obiskovalec dejansko na spletni strani na katero je imel namen priti.

Preverjanje podpisov in veriga zaupanja

Za potrebe digitalnih podpisov se ustvari par ključev, sestavljen iz zasebnega in javnega ključa (asimetrična kriptografija). Zasebni ključ je tajen in ostaja pri lastniku. Javni ključ se objavi v DNS-u kot DNSKEY zapis.

Z javnim ključem je tako možno preveriti veljavnost podpisa, ki je bil podpisan z zasebnim ključem.

Javnemu ključu moramo zaupati, ker z njim preverjamo podpisane DNS zapise. Za ta namen je ustvarjena “veriga zaupanja” - hierarhija podobna DNS hierarhiji.

Za podpisane domene se javni ključ prenese eno raven višje. Višja raven (parent) si zapiše javni ključ v svojo cono kot DS zapis in zagotavlja avtentičnost zapisa nižje ravni (child), tako da ga podpiše s svojim zasebnim ključem.

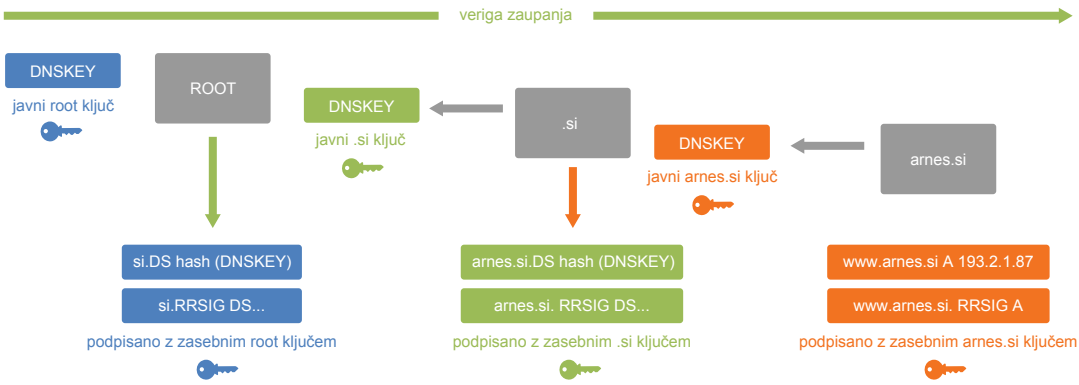
Kako začeti?

Povprečnemu uporabniku interneta pravzaprav ni potrebno storiti veliko. V kolikor ponudnik interneta podpira DNSSEC, bodo vsa preverjanja podpisov potekala na njihovih DNS strežnikih.

Če ste nosilec domene pa bo skrbnik vaše domene moral poskrbeti za ustrezno DNSSEC konfiguracijo. Na začetku DNSSEC najverjetneje ne bo zelo razširjen, predvidevamo da ga bodo uporabljale večinoma stranke, katerim je varnost visoko na seznamu prioritet (npr. banke).

Konec leta 2011 je bila vrhnja domena .si podpisana, prav tako se je sklenila tudi veriga zaupanja. IANA je dodala DS (Delegation Signer) zapise v root strežnik in s tem vzpostavila verigo zaupanja od root strežnikov do .si strežnikov. V letu 2012 bo register začel sprejemati DS zapise .si domen, ki bodo podpisane z DNSSEC.

Več o DNSSEC-u za .si domene si lahko preberete na strani http://www.register.si/dnssec



Slika 3: DNSSEC podpiše DNS zapise in nam s tem omogoči preverjanje avtentičnosti zapisov v DNS.

Akademska in raziskovalna mreža Slovenije (Arnes) je od svoje ustanovitve s strani IANA (Internet Assigned Names Authority) in Vlade RS pooblaščena organizacija za registracijo domen pod vrhnjo domeno .si in upravljanje vrhnjega DNS-strežnika za .si – register za vrhnjo domeno .si.

Arnes, p. p. 7, 1001 Ljubljana
T: 01 479 88 00, F: 01 479 88 99
E: dnssec@register.si
www.register.si
---
izdal: Arnes; uredil: Milijan Pružarev; oblikovanje: studio Zadruga; Ljubljana, december 2011