RASPODIJELJENI SUSTAV ZA UPRAVLJANJE DOMENSKIM NAZIVIMA TEMELJEN NA MREŽI RAVNOPRAVNIH ČVOROVA

Krešimir Pripužić, Valter Vasić
Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva,
Unska 3, 10000 Zagreb, Hrvatska
{kresimir.pripuzic, valter.vasic}@fer.hr
+385 1 6129 745

Sažetak – *U radu se daje osvrt na postojeći sustav DNS te se identificiraju njegovi nedostaci. Osim toga, opisuju se mreže ravnopravnih čvorova s posebnim osvrtom na strukturirane mreže. Na kraju se predlaže i detaljno opisuje sustav DNS koji se temelji na mreži ravnopravnih čvorova. Ovaj sustav je kompatibilan s postojećim sustavom DNS i rješava prethodno identificirane probleme standardnog sustava DNS.*

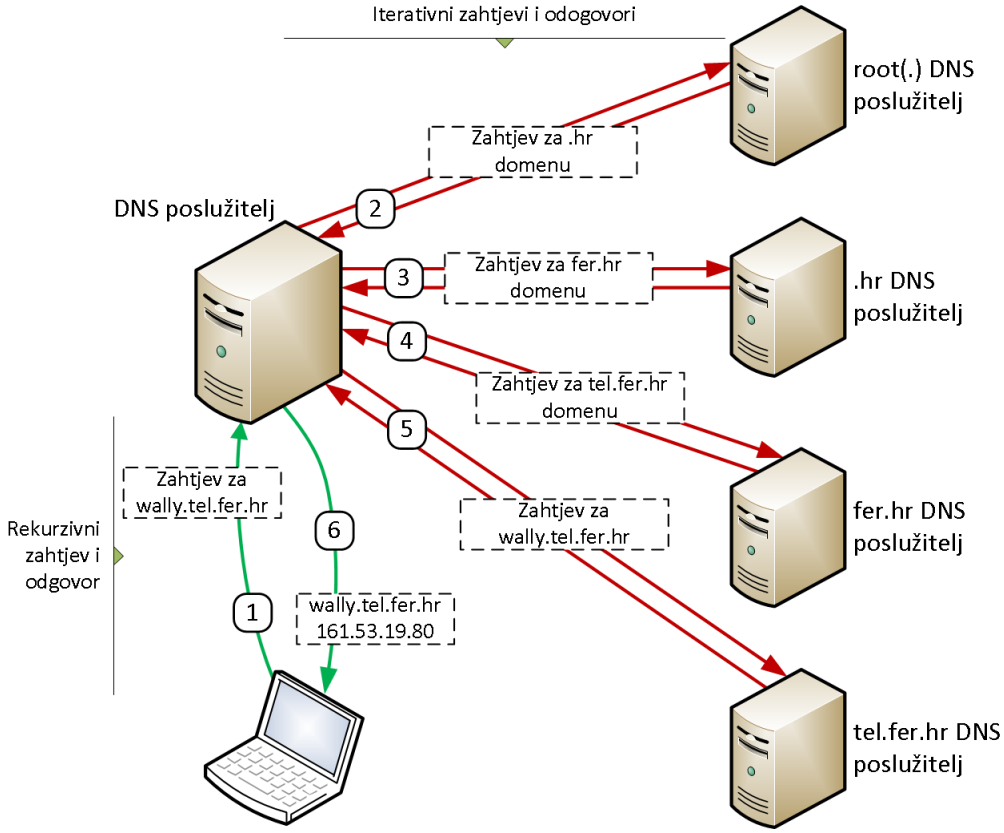
1. Uvod

U današnjem Internetu postoje brojni sigurnosni rizici. Čak i kada je računalo zaštićeno, na njega i dalje može dospjeti zlonamjeran softver od strane sustava koje koristimo u svakodnevnom radu. Jedan takav sustav je DNS sustav. Većina korisnika nije svjesna da se u sklopu Interneta koriste IP adrese, a ne samo nazivi računala. Današnji Internet bez sustava DNS bi bio nezamisliv zato što praktično svi današnji programi i usluge koriste DNS kako bi se pojednostavile migracije ili ugradili zalihosni mehanizmi. Isto se odnosi i na elektroničku poštu koja je također ovisna o sustavu DNS.

2. Sustav domenskih naziva

Sustav domenskih naziva DNS (*Domain Name System*) [4] jedna je od osnovnih servisa suvremenog Interneta. Prilikom komunikacije među čvorovima u Internetu najčešće se prije komunikacije dohvaća adresa čvora prema njegovom nazivu. Da bi se ona dohvatila nužno je slijediti hijerarhiju u nazivu čvora. Slijedeći hijerarhiju redom se komunicira s čvorovima nadležnim za pojedine domene, odnosno pod-domene. Da bi računalo u sklopu Interneta uspješno dohvatilo adresu računala s kojim želi započeti komunikaciju, ono mora imati pristup DNS poslužitelju. DNS poslužitelj će na vratima UDP 53 prihvaćati dolazne zahtjeve od klijenata te odgovarati adresama traženih domenskih naziva.

Na slici 1. vidljiv je postupak dohvaćanja IP adrese računala wally.tel.fer.hr s računala korisnika. Računalo prije svega šalje rekurzivni zahtjev svojem primarnom DNS poslužitelju, koji je lociran kod u lokalnoj mreži računala ili u mreži pružatelja Internet usluga (ISP). DNS poslužitelj će zatim umjesto klijenta iterativno dohvatiti adresu traženog čvora.



Slika 1 - Dohvaćanje adrese putem standardnog sustava DNS

Sljedeći koraci detaljno opisuju iterativno dohvaćanje adrese putem standardnog sustava DNS:

1. Od korijenskog DNS poslužitelja traži se adresa hr DNS poslužitelja,
2. Od hr DNS poslužitelja zahtijeva se adresa fer.hr DNS poslužitelja,
3. Od fer.hr DNS poslužitelja traži se adresa tel.fer.hr DNS poslužitelja,
4. Konačno od tel.fer.hr DNS poslužitelja zahtijeva se adresa računala pod imenom wally.

Nakon uspješnog dohvaćanja adrese, DNS poslužitelj odgovara traženom adresom na rekurzivni zahtjev klijenta.

2.1 Nedostaci sustava DNS

DNS poslužitelji su potencijalno jedne od glavnih meta napada u Internetu. Glavna prednost ovakvog napada je u tome da će u slučaju uspješnog napada sva računala koja koriste taj DNS poslužitelj mogu biti preusmjerena na štetna web sjedišta, a ona ih potencijalno mogu zaraziti nekakvom vrstom zlonamjernog softvera i/ili tražiti povjerljive podatke od korisnika. Najzastupljeniji napadi na DNS poslužitelje su sljedeći [5]:

- *DNS server buffer overflow* - iskorištavanje ranjivosti u kodu DNS poslužitelja koji omogućuje neautorizirani pristup DNS poslužitelju i izmjenu podataka na njemu.
- *DNS cache poisoning* - punjenje DNS međuspremnika lažnim unosima. [6]
- *Denial of Service* (DoS) - napad uskraćivanjem usluge, izvršava se onesposobljavanjem računala na kojem se izvodi DNS ili rušenjem servisa DNS na tom računalu. Podvrsta tog napada je DDoS (*Distributed* DoS), odnosno raspodijeljeni DoS.

Jedan od osnovnih nedostataka postojećeg DNS sustava je centraliziranost njegove arhitekture koja značajno utječe na smanjene njegove dostupnosti i robusnosti. DNS poslužitelji u svojim odgovorima daju podatke o tome na kojim se IP adresama nalaze svi DNS poslužitelji zaduženi za tu domenu. Ovo otkrivanje stoga uvelike olakšava napad na DNS poslužitelje za pojedinu domenu. Robusnost se može povećati s multipleksiranjem [7] na IP sloju, ali se u slučaju DoS napada takav sustav neće uspjeti obraniti. Ukoliko DNS poslužitelj ima ranjivosti u implementaciji potencijalni napadač vrlo jednostavno može učiniti poslužitelje nedostupnima, a da ona pri tome ne ovisni o broju poslužitelja. Dok je DNS poslužitelj javno dostupan i napadač može se doći do njegove IP adrese, kao što je trenutno slučaj, uvijek postoji mogućnost napada koji će onemogućiti njegov rad.

3. Mreže P2P čvorova

Mreže ravnopravnih čvorova (*peer-to-peer network, P2P network*) se najčešće spominju u kontekstu raspodijeljene razmjene datoteka na Internetu. Ovo je razumljivo s obzirom da većina današnjeg prometa na Internetu upravo otpada na navedenu razmjenu datoteka posredstvom mreža P2P. U narednim godinama se također predviđa nastavak dominacije prometa putem mreža P2P, u odnosu na ostale vrste Internetskog prometa, zbog sve veće popularnosti prijenosa stvarno-vremenskog video sadržaja posredstvom ovih mreža.

U odnosu na centralizirane sustave, glavne prednosti raspodijeljenih sustava temeljenih na mrežama P2P su samoorganizacija te povećana robusnost i pouzdanost. Samoorganizacija mreža P2P se očituje u nepostojanju centraliziranog koordinatora niti potrebi za ručnim namještanjem postavki sustava. Kako mreže P2P nemaju jedinstvenu točku ispada, samim time postižu značajno veću pouzdanost u odnosu na centralizirane sustave. Direktna posljedica navedenog je i povećana robusnost, tj. otpornost na kvarove, jer u slučaju kvara ispravni čvorovi mogu preuzeti zadaće neispravnih čvorova.

Mreže P2P možemo grubo podijeliti na strukturirane i nestrukturirane. Usmjeravanje poruka u nestrukturiranim mreža se vrši kontroliranim preplavljivanjem mreže u svrhu pronalaska traženog podatkovnog objekta. Nestrukturirane mreže P2P nemaju definiranu mrežnu topologiju te su jedini mogući načini usmjeravanja u ovim mrežama: preplavljivanje, slučajan izbor i prstenasto pretraživanjem s ograničenim parametrom TTL (*time to live*) u zaglavlju paketa IP. Za razliku od nestrukturiranih mreža P2P, strukturirane imaju definiranu mrežnu topologiju na način da čvorovi međusobno tvore strukturirani graf. Kod ovih mreža se za svaki podatkovni objekt može jednoznačno utvrditi kojem čvoru je on pridijeljen te se stoga usmjeravanje poruka vrši jednoznačno i deterministički. U slučaju ovih mreža, podatkovni objekti su pohranjeni na točno određenom čvoru, a ne nekom slučajno odabranom, čime se povećava učinkovitost pretrage za objektima koji su pohranjeni u mreži. Štoviše, ove mreže garantiraju pronalazak svakog postojećeg objekta u $O(\log n)$ koraka, gdje je n ukupan broj čvorova u mreži. Svakom novom podatkovnom objektu se pri tome dodjeljuje jedinstveni ključ te se prilikom dodavanja u mrežu objekt pohranjuju na čvor koji je zadužen za taj ključ.

Strukturirane mreže P2P se najčešće koriste kao raspodijeljene tablice s raspršenim adresiranjem (*Distributed Hash Table*, DHT). Ove tablice omogućavaju raspodijeljenu pohranu parova ključ-vrijednost unutar mreže P2P, a pri tome nasljeđuju sve prethodno navedene prednosti ovih mreža. Tri najpopularnija DHT-a su sljedeće mreže P2P: Chord [1], CAN [2] i P-Grid [3]. Mreža Chord organizira čvorove u obliku prstena u kojem, osim veza među susjednim čvorovima u prstenu, također postoji dovoljan broj veza unutar samog prstena čime se osigurava brzo pronalaženje traženog podatkovnog objekta. Svaki čvor u mreži Chord je zadužen za slijedni niz cjelobrojnih ključeva (i njima pridijeljenih podatkovnih objekata) koji čini podskup konačnog broja ključeva u mreži. Za razliku od mreže Chord, mreža CAN podržava beskonačan broj ključeva u obliku n-torki realnih brojeva, gdje je n dimenzija atributnog prostora ključeva. Drugim riječima, kod mreže Chord

je broj ključeva konačan dok je kod mreže CAN konačan broj dimenzija ključeva. U mreži P-Grid čvorovi su organizirani u binarno stablo u kojem ne postoji hijerarhija čvorova jer je struktura stabla raspodijeljena među čvorovima. Osim toga, ova mreža podržava neograničen broj cjelobrojnih ključeva te se izvrsno prilagođava unaprijed nepoznatoj raspodjeli njihovih vrijednosti. Zbog svojih dobrih karakteristika, mreže P-Grid se pokazuje puno boljom za izgradnju sustava domenskih naziva od mreža Chord i CAN.

4. Sustav domenskih naziva zasnovan na P2P mreži

Raspodijeljeni sustav DNS koji predlažemo u ovom poglavlju koristi mrežu P-Grid [3]. Uporaba ove strukturirane mreže P2P za ostvarivanje DNS sustava ima sljedeće prednosti:

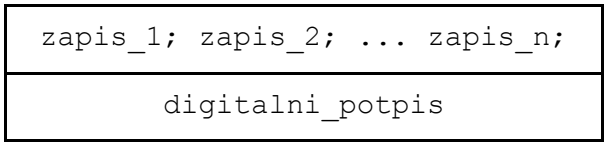
- Decentraliziranost i nepostojanje hijerarhije - onemogućuje se cenzuriranje i sprječavanje mogućnosti javnog govora putem sustava DNS.
- Robusnost - manja mogućnost ispada sustava DNS.
- Veću razinu sigurnosti - teže dolaženje do informacija o čvorovima u P2P mreži. Svi čvorovi koji nisu susjedni su međusobno anonimni.
- Zadržavanje kompatibilnosti s postojećim sustavom DNS.

Za pohranjivanje parova naziv-adresa te dohvaćanje adrese na osnovu naziva se koriste metode raspodijeljenog raspršenog adresiranja unutar mreže ravnopravnih čvorova. Nakon što određeni čvor objavi zapis `naziv:IP_adresa`, ova poruka se anonimno širi kroz mrežu i pronalazi čvor koji je zadužen za taj naziv. Ovaj čvor pohranjuje zapis u svoju lokalnu bazu podataka da bi bio u stanju poslužiti naknadne korisničke upite.

Slično pohrani para naziv-adresa vrši se pronalaženje adrese na osnovu naziva. Nakon što neki čvor zatraži otkrivanje adrese na osnovu naziva, ova poruka se širi kroz mrežu i pronalazi čvor koji je zadužen za taj naziv. Potom taj čvor čita adresu iz lokalne baze podataka i prosljeđuje odgovor čvoru. Poput poruke upita i pohrane novog para, ovaj odgovor se također anonimno širi kroz mrežu P2P čime se onemogućava otkrivanje čvora koji je bio zadužen za ovaj naziv. U slučaju da naziv nije pronađen onda se prelazi na standardan način dohvaćanja IP adrese prema nazivu posredstvom standardnog sustava DNS.

4.1 Format poruke i sigurnosne mjere

Format zapisa koji se koristi prilikom prijenosa para naziv-adresa putem mreže P2P prikazan je na Slici 2.



Slika 2 - Format poruke za prijenos domenskog zapisa

Digitalni potpisom se osigurava cjelovitost sadržaja poruke. Digitalni potpis je asimetrično šifrirani sažetak (generiran pomoću kriptografske *hash* funkcije) sadržaja poruke. Pošiljatelj šifrira poruku svojim privatnim ključem, dok će primatelji provjeriti ispravnost poruke ponovnim generiranjem sažetka i njegovom usporedbom s dešifriranim sažetkom iz potpisa.

Vjerodostojnost poruke kojom unosi/mijenja par naziv-adresa utvrđuje se kod odredišnog čvora kroz tablicu koja sadrži nazive domena i pripadne javne ključeve za provjeru valjanosti digitalnog potpisa. Primjer parova domena-javni ključ je vidljiv u Tablici 1. Ukoliko provjera valjanosti digitalnog potpisa nije uspjela zahtjev za zapisom se odbacuje.

Naziv domene	Javni ključ
marko.hr	mQCNAi+UeBsAAAEEAMP0kXU7...
kreso.com	tB5NYXJ0eSBNY0ZseSA8bWFy...

Tablica 1 - Javni ključevi i nazivi domena

Za digitalni potpis koriste se kriptografske funkcije novije generacije, za funkciju sažetka barem SHA-256 (SHA-2 algoritam sa duljinom sažetka od 256 bita), a za asimetričnu kriptografiju barem RSA-1024 (RSA algoritam sa duljinom ključa od 1024 bita). Ovime se osigurava dovoljna razina sigurnosti prilikom komunikacije u sustavu.

4.2 Proširenja postojećeg sustava i budući rad

Ukoliko je tablica parova naziv_domene-javni_ključ postavljena prije prvog korištenja sustava, cijeli sustav se može koristiti bez opasnosti od štetnih unosa. U suprotnom je potrebno pri prvom unosu adrese domene zabilježiti naziv domene i odgovarajući javni ključ u tablicu. Ukoliko je početni unos štetan javlja se problem njegovog jednostavnog uklanjanja iz tablice. Da bi se takvi unosi spriječili može se uvesti sustav reputacije i glasanja čime se na brz i efikasan način mogu ukloniti štetni unosi.

Uz to ovakav sustav se može spojiti s infrastrukturom javnog ključa (PKI) kroz koju bi se mogla ostvariti provjera identiteta čvorova pomoću javnog ključa i time dodatno osigurati cjelokupan sustav.

4.3 Usporedba sa standardnim sustavom DNS

U Tablici 2 je dana pregledna usporedba prednosti i nedostataka standardnog sustava DNS sa sustavom domenskih naziva temeljenim na mreži P2P. Kao što se vidi u tablici, jedini identificirani nedostatak sustava DNS temeljenog na mreži P2P je potreba za prilagodbom organizacije sustava prilikom dodavanja i uklanjanja poslužitelja iz mreže (promjenjivost sustava). Međutim, kako je očekivana frekvencija promjena poslužitelja u sustavu DNS vrlo niska, ovaj nedostatak neće značajno utjecati na odziv sustava.

	Organizacija sustava	Brzina odgovora	Vjerodostojnost sustava	Raspoloživost sustava	Promjenjivost sustava
Standardni sustav DNS	Hijerarhija centraliziranih poslužitelja	Spor odziv, višestruki upiti	Niska razina (bez DNSSEC)	Nema garancije (mogućnost izravnog ciljanog napada)	Ručno definirana organizacija, trenutne promjene
Sustav DNS temeljen na mreži P2P	Decentralizirani sustav	Brz odziv, jedan upit	Proizvoljna razina sigurnosti	Arhitektura mreže onemogućava izravan ciljani napad	Sporija automatizirana prilagodba

Tablica 2 – Usporedba karakteristika standardnog i P2P sustava DNS

5. Zaključak

U ovom radu se daje prijedlog sustava DNS koji se temelji na mreži ravnopravnih čvorova P-Grid, a kompatibilan je s postojećim sustavom DNS. Ovaj sustav rješava glavne nedostatke standardnog sustava DNS, a to su smanjena robusnost i pouzdanost zbog centralizirane strukture te sigurnosni nedostaci koji su posljedica hijerarhijske organizacije. Uz to se dodatno osigurava automatiziran unos i održavanje domenskih zapisa kroz mrežu ravnopravnih čvorova, bez narušavanja kompatibilnosti. Pristup predloženom sustavu se može osigurati putem lokalnog DNS poslužitelja koji bi umjesto standardnog iterativnog dohvaćanja IP adrese koristio dohvaćanje putem predloženog sustava.

Popis literature

1. I. Stoica, R. Morris, D. Karger, F. Kaashoek, and H. Balakrishnan, “Chord: A Scalable Peer-To-Peer Lookup Service for Internet Applications”, In Proceedings of the 2001 ACM Sigcomm Conference, pp. 149–160, ACM Press, 2001.

2. S. Ratnasamy, P. Francis, M. Handley, R. M. Karp, and S. Shenker, “A Scalable Content-Addressable Network”, In SIGCOMM, pp. 161–172, ACM Press, 2001.

3. K. Aberer, P. Cudr´e-Mauroux, A. Datta, Z. Despotovic, M. Hauswirth, M. Punceva, and R. Schmidt, “P-Grid: A Self-organizing Structured P2P System”, ACM SIGMOD Record, 32(3), 2003.

4. P. Mockapetris, “DOMAIN NAMES - CONCEPTS AND FACILITIES”, IETF, RFC 1034, 1987.

5. Security Associates Institute, “Attacking the DNS Protocol”, 2003.

6. C. Racki, “DNS cache poisoning”, 2008.

7. Heon Y. Yeom, Jungsoo Ha, & Ilhwan Kim, “IP Multiplexing by Transparent Port-Address Translator”, Tenth USENIX System Administration Conference, 1996.