Систем доменских имена са безбедносним проширењима – DNSSEC

Лозница, 2017.

САДРЖАЈ

1. Увод

Комуникација између различитих ресурса на Интернету се ослања на међусобно адресирање на основу Интернет протокол адреса (енгл. *Internet Protocol address*). Различити ресурси на Интернету имају јединствене адресе у виду бројева који су подељени у четири октета (8 битова) растављених тачкама, односно четири октета са бројевима од 0 до 255. Људима је природно да памте називе, због чега су адресе у виду бројева замењене називима тих ресурса што је омогућено увођењем система доменских имена, DNS (енгл. *Domain Name System*). Овај систем је задужен за превођење IP адреса у доменска имена, односно за повезивање доменских имена са одговарајућим IP адресама. Заснива се на клијент сервер архитектури где клијентски део представља DNS разрешитељ (енгл. *DNS resolver*) који је интегрални део мрежног софтвера и који је задужен за слање упита о томе која IP адреса одговара ком доменском имену (енгл. *Domain Name*) и других података у вези са конкретним ресурсом. Северски део се налази у саставу софтвера DNS севера и има задатак да снабдева подацима клијентски део у комуникацији, уколико су задовољени сви постављени услови.

Систем доменских имена је у периоду од петнаест година функционисао без већих проблема, ако се изузме недовољно брзо ажурирање података DNS записа и уколико се изузме рањивост система на измену података о DNS записима. Подаци који се транспортују путем Интернета се усмеравају зависно од полазишта и коначног одредишта, при чему су датотеке које се транспортују подељене у мање целине, односно у пакете података који се транспортују независно и који не морају ићи изворним редоследом и једнаким путањама од полазишта до одредишта. Обзиром да је DNS имплементиран тако да аутоматски регулише повезивање предајне и пријемне стране и обзиром да у основи нема безбедносне механизме, потенцијални нападачи имају релативно велики простор да искористе безбедносне пропусте.

DNS напади се односе на компромитовање система којим се врши превођење словног записа назива (симболичка адреса) неке станице на Интернету, односно имена домена, у бинарни запис, односно Интернет протокол адресу (логичка адреса). Интернет клијенти комуницирају са дистрибуираном базом података на DNS серверима и када неки од сервера нема податке, односно нема могућност мапирања жељеног захтева, односно повезивања имена домена и IP адресе, он прослеђује тај захтев другом блиском DNS серверу. Том приликом, сервер који је упутио захтев архивира нову путању мапирања како би се она могла користити приликом будућих упита у наредном временском периоду. Одсуство аутентификације сервера и клијента представља безбедносни ризик и омогућава нападачима да убеђују или да убеде клијенте да је повратна порука аутентична и да их тако усмере ка лажним Интернет ресурсима. DNS напад се може извести на разним местима у комуникационом ланцу. Када нападач приступи DNS бази података он је у могућности да измени одређени запис, или групу записа и да преусмери будуће клијентске захтеве на лажну Интернет адресу ка лажној Интернет апликацији која у свему подсећа на оригиналну и да тако злоупотреби поверење корисника те апликације. Наравно, Интернет се заснива и на другим системима који у одређеној мери повећавају ниво безбедности, првенствено на SSL (енгл. *Secure Socket Layer*) протоколу и на његовом наследнику TLS (енгл. *Transport Layer Security*) протоколу, међутим шифровање комуникације не решава проблем аутентификације DNS сервера, као посредника у комуникацији, што представља безбедносни ризик.

2. Систем доменских имена – DNS

Седамдесетих година прошлог века, Америчко Министарство одбране (енгл. *United States Department of Defense*) је донело одлуку за креирање компјутерске комуникационе мреже. Реализација те мреже је поверена организацији Министарства одбране Сједињених Америчких Држава за развој нових војних технологија, односно DARPA (енгл. *Defense Advanced Research Projects Agency*) по чијем имену је, након реализације, та мрежа добила име: ARPAnet. Данас се ова мрежа сматра претечом Интернета јер је њеном реализацијом направљен и нови протокол који је дефинисао пакетски пренос података, адресирање мрежних уређаја на основу IP адреса, одређивање оптималних путања за слање података, комуницирање између различитих компјутерских мрежа и између различитих типова уређаја повезаних на мрежу. Убрзо након реализације ове мреже постале су очигледне њене могућности и бројне предности које пружа овакав вид комуникације. То је довело до њеног наглог развоја, а затим и до реализације Интернета, мреже коју данас познајемо.

Први проблем на који је наишао ARPAnet био је у вези са наглим порастом броја уређаја које је требало повезати, односно адресирати. Тај проблем је превазиђен захваљујући решењима које је понудила организације под називом IANA (енгл. *Internet Assigned Numbers Authority*). Ова организација је проблеме адресирања уређаја на мрежи решила кроз достизање неколико циљева. Ти циљеви су били у вези са глобалним надзором расподеле IP адреса, затим у вези са реализацијом и управљањем системом доменских имена и доношењем и реализацијом бројних стандарда везаних за бројеве и симболе у Интернет протоколу. Почетно су уређаји били адресирани искључиво нумеричким адресама, међутим то није било адекватно решење обзиром на промену типа корисника Интернета, односно на пораст боја корисника и обзиром на то да је Интернет, поред едукативне и истраживачке сврхе, све више добијао на значају као средство у пословном посредовању, рекламирању, забави и слично. Ускоро након тога, 1984. године је реализован DNS чиме је адресирање уређаја на мрежи добило данашњи облик.

Даљи развој Интернета је омогућен појавом приватних Интернет провајдера, 1991. године, и појавом приватних организација за регистрацију Интернет домена, 1992. године, које су пословале по законима тржишне економије што је довело до значајног смањења цена услуга. Након формирања компаније под називом ICANN (енгл. *Corporation for Assigned Namesand Numbers*), 1998. године, централизована је координација функционисања и развоја Интернета на глобалном нивоу. Њеним оснивањем је, у институционалном смислу, омогућена сарадња заинтересованих страна да учествују у стварању и да спроводе регулативу у вези са функционисањем и развојем Интернета. Такође, ICANN је омогућио акредитовање великог броја организација које корисницима омогућавају регистрацију нових домена. Тако је створен Заједнички систем за регистрацију домена (енгл. *Shared Registration System*) и омогућена је децентрализована регистрација домена у складу са регулативном политиком и у складу са законима тржишне економије.

Први кораци у адресирању мрежних уређаја у мањим мрежама је реализовано на као систем где су подаци о именима уређаја чувани у host датотекама које су се физички налазиле на тим уређајима, односно компјутерима. То је било доста непрактично решење јер није било могуће једноставно изменити податке о адресама уређаја. Овај недостатак је превазиђен новим системом који је користио дистрибуиране host

датотеке, а након тога и дистрибуиране базе података. Стари системи са host датотекама још увек могу бити алтернативно решење за DNS и могу се применити у мањим локалним мрежама уз аутоматске софтверске, или мануелне, односно ручне измене садржаја тих фајлова. Када су у питању веће мреже, адресирање компјутера уз помоћ host фајлова је непрактично, поред тога што је потребно мењати њихов садржај на свим компјутерима уколико дође до промене броја компјутера, њиховог назива, или адресе у мрежи, овакав систем је доста спорији од система доменских имена. Данас у великим мрежама попут Интернета, систем за именовање уређаја чине хијерархијски повезани DNS сервери од којих је сваки појединачно, или свака група задужена за чување, обраду и давање информација о наведеним доменима.

DNS какав данас познајемо је настао дугогодишњим развојем, а према истраживањима из 2015. године, процењује се да је путем Интернета, посредством провајдера у оквиру бројних локалних мрежа, повезано више од осам милијарди уређаја. Чување тако велике количине података представља сложен технички изазов јер у сваком тренутку постоји велики број захтева за добијање података на основу којих ће се успоставити веза између конкретних мрежних уређаја, поред чега подаци који обезбеђују повезивање нису статични већ се непрестано мењају у времену. DNS је имплементиран као глобално дистрибуирана, хијерархијски организована и динамички оријентисана база података. Ово омогућава да се релативно велика количина података дистрибуира на релативно велики број сервера тако што се на свим DNS серверима чува део података који се чешће захтевају и који се ажурирају у предвиђеним временским интервалима, или у зависности од клијентских захтева. Имајући у виду непрестано повећање броја уређаја повезаних путем Интернета, DNS базе су реализоване тако да постоји могућност непрестаног додавања записа о новим ресурсима.

Систем доменских имена је организован хијерархијски тако да за сваку ставку и сваки ниво постоји запис у DNS серверу надлежном за ту зону доменских имена. Сваки надлежни DNS сервер (енгл. *Authoritative Name Servers*) располаже подацима за ту зону и за зоне које се налазе на хијерархијски нижем нивоу. Приликом слања захтева за неким доменом, серверски софтвер за разрешавање тог захтева рекурзивно покушава да дође до података које чувају сервери, а након тога их повезује у комплетан назив домена, односно повезује име жељеног ресурса на Интернету са његовом IP адресом. Назив домена се састоји од, најмање, два дела раздвојених тачкама. Посматрано са десне стране ка левој, први део представља назив највишег домена, а сваки наредни део представља назив поддомена највишег домена, односно поддомен првог надређеног домена. На самом врху хијерархије домена се налази основни домен (енгл. *Root Domain*) који се означава тачком „.“. На њега се надовезује домен највишег нивоа, односно TLD (енгл. *Top Level Domain*) који, у зависности од прихваћене поделе, може бити TLD везан за државе, на пример: *rs* – Република Србија, *ru* - Руска Федерација, или *de* - Савезна Република Немачка, затим генерички TLD који се користи за одређену категорију организација, на пример: *com* – за комерцијалне организације, *edu* – за едукативне организације, *coop* – за невладине организације, или *museum* – који је предвиђен за музеје. Следеће, ниже подручје у односу на TLD представљају домени другог нивоа, односно SLD (енгл. *Second Level Domain*) и те домене могу регистровати правна и физичка лица под условом да ти домени нису већ у употреби. На следећем, најнижем подручју у односу на домене другог нивоа, налазе се поддомени (енгл. *Subdomain*). Поддомен се може произвољно додати испод већ регистрованих домена.

Поред наведених домена највишег нивоа постоји и инфраструктурни домен највишег нивоа, *arpa* домен. Његови домени другог нивоа имају различите функције, na пример *in-addr.arpa* и *ip6.arpa* омогућавају обрнуто мапирање (енгл. *Reverse DNS Lookup*), односно проналажење имена компјутера на основу његове IP адресе. Обрнуто мапирање је практично у борби против слања нежељене поште (енгл. *Anti Spam techniques*). Техника филтрирања се заснива на провери логичности назива домена добијених из IP адреса сервера који шаљу пошту. Примера ради, домен *dynamic-ip.com*, не би задовољио очекиване критеријуме. Такође, обрнуто мапирање омогућава да се направи верификација која проверава да ли постоји унапред дефинисан пар доменског имена и одговарајуће IP адресе, односно FCrDNS (енгл. *Forward Confirmed Reverse DNS*). Иако оваква провера не представља вид идентификације сервера, довољно је добар начин да се сервер нађе на листи привилегованих, односно пожељних (енгл. *Whitelist*). Поред домена који служе обрнутом мапирању, постоје *uri.arpa* и *urn.arpa* за апликације које користе DNS заснован на DDDS (енгл. *Dynamic Delegation Discovery System*) најчешће у Интернет телефонији, или *e164.arpa* за мапирање бројева телефона.

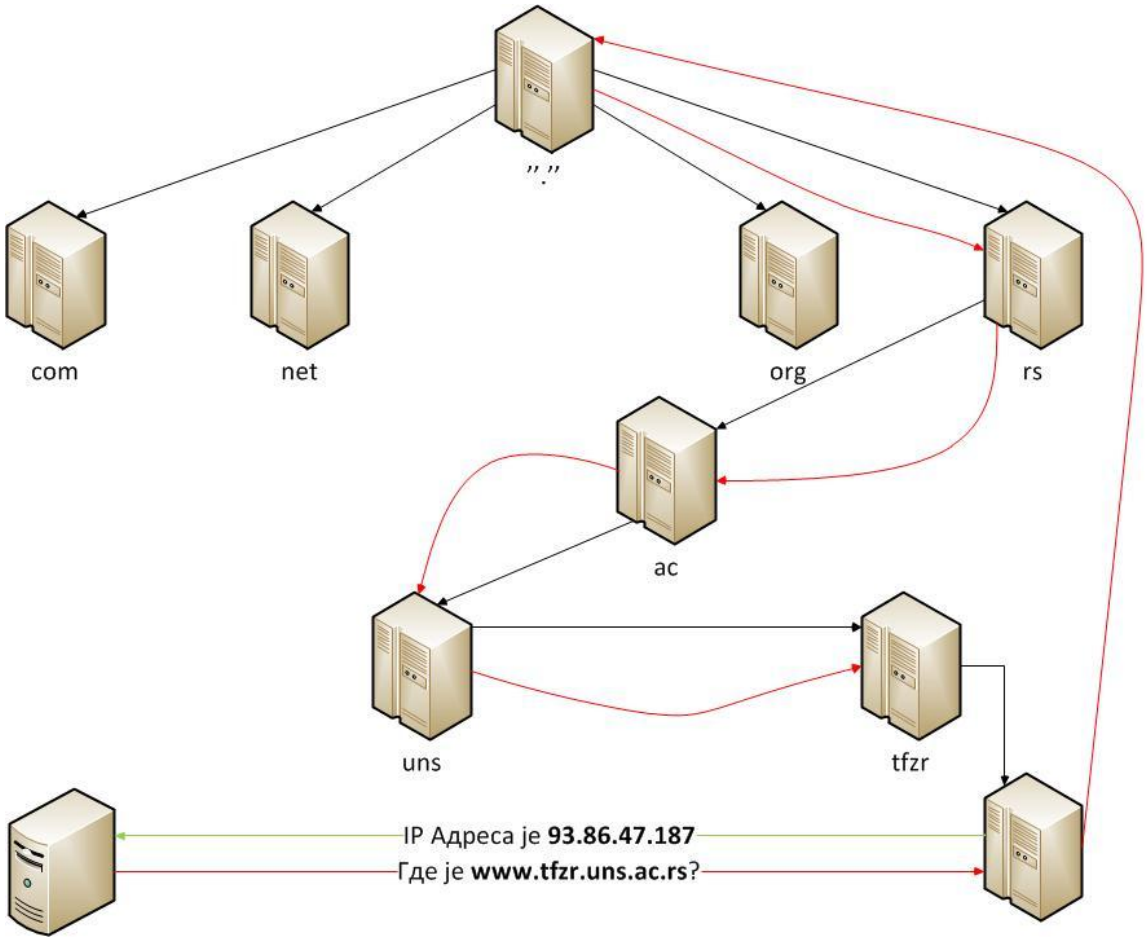
2.1 Начин рада DNS сервера

DNS сервери могу бити ауторитативни и неауторитативни. Ауторитативни DNS сервери чувају податке о адресама мрежних уређаја у локалним датотекама које није једноставно компромитовати због чега се ти подаци сматрају тачним и представљају извор из ког се снабдевају остали DNS сервери. Неауторитативни DNS сервери до података о вези између IP адреса и доменских имена долазе на основу информација које добијају од ауторитативних DNS сервера, након чега могу да међусобно размењују информације о адресама различитих ресурса на Интернету. За сваки домен постоје најмање два ауторитативна DNS сервера који чувају податке о њему. Њихов задатак је да одговарају на упите који се односе на наведени домен и на остале податке у вези са тим, док се сами подаци организовани у записе о тим ресурсима, RR (енгл. *Resource Record*), односно у зонске датотеке.

Ауторитативни DNS сервери могу бити примарни, који је само један, и секундарни, којих може бити више. Како би се обезбедила контрола над подацима, процес њиховог ажурирања се реализује тако што се подаци у табелама директно ажурирају само на примарном DNS серверу, на основу протокола за динамичку измену података у зонској датотеци којима може да приступи DHCP (енгл. *Dynamic Host Configuration Protocol*) север и да дода, измени, или обрише записе. Након ажурирања података на примарним аутоматски се ажурирају подаци у табелама на секундарним DNS серверима. По учитавању података у вези са одређеним доменом, примарни сервер шаље поруку свим секундарним серверима, након чега сви секундарни сервери могу да затраже пренос комплетне табеле са подацима, или пренос само нових података у вези са наведеним доменом. На овај начин се обезбеђује синхронизација података на примарном и секундарним DNS серверима. Поред овог начина за креирање и трансфер новог зонског фајла на секундарни DNS сервер, подаци се могу освежити мануелно, или и тако што ће се подесити аутоматско ажурирање. У оквиру првог записа у свим зонским датотекама, SOA (енгл. *Start of Authority*) постоји податак о томе у ком временском интервалу ће секундарни сервер проверити да ли је на примарном серверу дошло до повећања сиријског броја записа о доменима (енгл. *Start of Authority Resource Record*). Уколико секундарни DNS сервер не добије одговор на свој упит, поновиће га након истека

времена, а уколико истекне период након кога се претпоставља да неки домен више није активан, секундарни DNS сервер ће обрисати податке о конкретним доменским именом.

Све мрежне апликације које пре приступају неком од ресурса путем Интернета шаљу DNS упит за добијање IP адресе мрежног уређаја са којим треба да успоставе комуникацију. Ти упити могу да буду итеративни, или рекурзивни зависно од тога да ли упитани DNS сервер има тражене податке, или не. Код итеративних упита, DNS сервер поседује све потребне податке које шаље на основу постављеног упита, док код рекурзивних упита контактирани DNS сервер не поседује тражене податке, па започиње рекурзивни поступак тражења захтеваних података. Рекурзивни поступак у основи подразумева да DNS разрешитељ шаље DNS упит серверу чију адресу аутоматски добија посредством DHCP сервера, а након што се утврди да конкретни DNS сервер не располаже траженим подацима, започиње постављање упита надређеним серверима док се не пронађе ауторитативни DNS сервер који располаже траженим подацима.



Слика 1 *Разрешавање доменских имена*

На пример, уколико клијентски компјутер не успе да пронађе потребне податке и приступи ресурсима везаним за домен *tfzr.uns.ac.rs*, односно уколико не пронађе ауторитативни сервер за овај домен, он ће послати поновни захтев серверу који се налази на вишем нивоу за домен *uns.ac.rs*, а уколико ни он не поседује потребне

податке, захтев ће бити прослеђен серверу вишег нивоа све док се не добију тражени подаци, или док се не контактира сервер највишег нивоа, основни DNS сервер (енгл. *Root DNS server*). Основни DNS сервер такође нема тражене податке, али зна који су ауторитативни DNS сервери за домен *rs*, након чега упит прослеђује тим серверима, који враћају податке о листи ауторитативних DNS сервера за домен вишег нивоа *ac.rs*, они, опет листу ауторитативних сервера за домен *uns.ac.rs*, након чега ће бити контактирани ауторитативни DNS сервери који поседују IP адресу мрежног уређаја на којој се налазе тражени ресурси везани за име домена *tfzr.uns.ac.rs*.

Након што неауторитативни DNS сервер добије одговор од ауторитативног DNS сервера он ту информацију смешта у сопствену кеш меморију након чега је прослеђује клијентском компјутеру који је послао упит. Кеширање података на неауторитативним DNS серверима значајно убрзава процес добијања IP адресе на основу доменског имена и сваки следећи клијентски захтев за приступање истом ресурсу ће бити брзо испуњен. Период у ком су кеширани подаци валидни зависи од подешавања, а податак о том подешавању чува сваки DNS сервер. Поред тога што неауторитативни DNS сервери чувају податке добијене од ауторитативних сервера и сам клијентски компјутер, односно неки други мрежни уређај, чува наведене податке у предвиђеном временском периоду.

2.2 Безбедносни недостаци система доменских имена

Систем доменских имена се није значајно променио од времена његовог настанка јер није постојао простор за његове модификације, првенствено због тога што је он интегрални део функционалности претраживања ресурса путем Интернета, која у основи подразумева да то буде систем са доступним сервисима и ресурсима. DNS је настао у периоду када је Интернет представљао средство комуникације између научних и истраживачких организација па је број потенцијалних нападача био релативно мали, међутим комерцијализацијом Интернета појавиле су се бројне интересне групе које нису бирале средства да остваре своје циљеве. Безбедносни проблеми који су се појављивали су парцијално решавани путем различитих софтверских модификација на DNS серверима, међутим још увек постоје бројни недостаци које је могуће злоупотребити. Уобичајена слабост свих Интернет система је могућност реализације DoS, или DDoS напада (енгл. *Denial of Service, Distributed Denial of Serivce*) која се ослања на суштинску функционалност свих система који раде захваљујући, или посредством Интернета, односно на томе да морају да реагују након што им се упуте захтеви. Уколико им се упути превелики број захтева у релативно кратком временском периоду, они ће, услед ограничености ресурса почети споро да реагују што ће довести до немогућности функционисања система, па самим тим и до немогућности реализације жељене услуге у времену у ком би то било сврсисходно.

Динамичко ажурирање података на DNS серверима је неопходно услед постојања велике количине података и услед релативно честих измена, међутим управо то отвара могућност да се у базе унесу неисправне, или лажне адресе што омогућава злоупотребу система тако што ће приказати неке од ресурса као аутентичне и ако су замењени лажним. Такође, обзиром да не DNS не поседује системе за шифровање, постоји могућност откривања података важних за безбедност DNS сервера, односно постоји могућност да се пресретне комуникација и да се клијентима проследе лажне IP адресе након чега би били усмерени на лажне сервере. Поред овога, одсуство

система за аутентификацију сервера омогућава потенцијалним нападачима да измене податке у кеш меморији DNS сервера (енгл. *Cache poisoning*) и тако преузму контролу након чега су у могућности да слањем нетачних података крајње кориснике усмеравају ка лажним серверима.

Набројани напади не морају увек да имају озбиљне последице, али уколико би неко намеравао да искористи безбедносне пропусте постојећег система доменских имена могао би да направи велике проблеме. На пример, када не би постојали додатни безбедностни системи потенцијални нападачи би могли измене записе на DNS серверима и да направе лажне Интернет апликације за куповину путем Интернета, или за реализацију банкарских послова. Када корисник унесе адресу банке, или сајта за куповину реко Интернета, услед нетачних података на DNS серверу он бива усмерен ка серверима где су постављене апликације које по изгледу и функционалности изгледају управо као оне које је навикао да користи, али које имају скривене програме који сакупљају тајне податке корисника. Корисници веома ретко проверавају адресе ресурса на интернету, односно URL (енгл. *Uniform Resource Locator*) и скоро никада не проверавају IP адресе тих ресурса, а управо то омогућава превару јер не постоји сумња у веродостојност апликације и корисници се понашају у складу са уобичајеним навикама и уносе тајне податке за аутентификацију са којима потенцијални нападач, након успешно реализоване преваре, може приступити финансијским средствима корисника и извршити трансакције по свом избору, или може у име корисника обавити неке од послова путем Интернета.

Лажне локације на Интернету могу омогућити ширење злонамерних апликација са циљем да се прикупљају подаци о корисницима у различите сврхе без њиховог одобрења, да се користе хардверски ресурси крајњих корисника, или да се у корисничким активностима сакрију неке од активности нападача. Уколико корисници са лажних сајтова преузму неку од модификованих верзија апликација коју намеравају да користе, могу постати жртве неког од оваквих напада. Обзиром да корисници, претежно, не користе хеш функције (енгл. *Hash functions*) за потврђивање интегритета поруке, односно апликација које преузимају, сценарио у ком користе неку од модификованих апликација је веома вероватан. Корисници самом употребом преузете апликације непрестано шаљу податке о свом понашању на Интернету, или своје личне податке, или уступају део хардверских ресурса нападачима, или, не слутећи ништа и сами постају нападачи.

Напади лажирања података на DNS серверима могу бити веома незгодни када су у питању масовни медији, нарочито у периодима политичких криза, или када су у питању географске области са нестабилном друштвеном ситуацијом. Уколико се становништву у таквим подручјима пласирају дезинформације, или информације могуће је остварити одређене утицаје. Овакве видове напада би могле да искористе велике маркетиншке агенције, различите структуре власти различитих држава, или организације супротстављених политичких партија. Обзиром да је у питању пласирање вести великом броју корисника, ово може бити злоупотребљено тако што би се грађани побудили на протесте, или би се умириле оправдане тензије због кршења њихових права, или тако што би им се пласирали производи, или услуге на основу пропаганде која у другачијим околностима не би могла да постигне довољно значајан утицај.

3. Безбедносна проширења система доменских имена - DNSSEC

Потенцијални нападачи могу, уз релативно мала улагања, пресрести неки од захтева који је прослеђен DNS серверу и преузети контролу над сесијом, након чега је могуће посматрати комуникацију и прикупљати, па и злоупотребити осетљиве податке о корисницима. Наравно, могуће је и открити такве активности, али оптимално решење за отклањање оваквих безбедносних претњи се налази у превентивном деловању, односно у развоју и имплементацији безбедносних проширења за DNS. Та проширења у комбинацији са Системом доменских имена чине Систем доменских имена са безбедносним проширењима, односно DNSSEC (енгл. *Domain Name System Security Extensions*). Ова технологија је развијена да делује превентивно када су у питању различити безбедносни ризици и она се заснива на дигиталном потписивању података.

DNSSEC представља оптимално решење за аутентификацију DNS сервера. Обзиром да DNSSEC технологија не подразумева шифровање података већ само дигитално потписивање одговора добијених од DNS сервера, а на основу захтева упућених од стране клијената, она обезбеђује добре перформансе уз мале трошкове. Међутим, у односу на DNS без безбедносних проширења, за функционисање DNSSEC – а је потребно више ресурса и више времена за одговор, односно за обраду и слање података. Дигитално потписивање је захтевно када је у питању процесорска снага. Количина података коју је потребно обрадити и транспортовати је од три до шест пута већа у односу на систем доменских имена без безбедносних проширења, поред тога, дистрибуција кључева представља специфичну проблематику. На то се надовезују проблематика администрације и проблематика контроле над тим ресурсом, односно контроле над DNSSEC – ом.

DNSSEC омогућава потврду аутентичности порекла података и интегритет података на употребом асиметричних криптографских алгоритама. Потпуна имплементација DNSSEC – а обезбеђује верификацију сервера и омогућава крајњим корисницима да се повежу на аутентични сервер, или да дођу до жељених аутентичних ресурса на основу доменског имена. Корисници при томе могу бити сигурни да одговор потиче од ауторитативног сервера задуженог за конкретну зону и да су добили тачну IP адресу. Такође, захваљујући дигиталном потписивању, ова технологија омогућава да се постигне интегритет одговора, односно потврда да одговор DNS сервера није мењан на свом путу. Са друге стране, DNSSEC не поседује систем заштите од онеспособљавања сервера или неких других виталних делова комуникационе инфраструктуре, односно не поседује систем заштите од DDoS напада. Такође, DNSSEC ни на који начин не поседује систем за проверу тачности DNS података, па иако је могуће сачувати интегритет података, то не мора нужно значити да су подаци тачни и да су DNS сервери правилно подешени.

Безбедносна проширења имплементирана у DNSSEC подразумевају додавање података у већ постојећи систем, у DNS. Потпис, односно SIG (енгл. *Signature*) је запис који је предвиђен за чување дигиталног потписа у Систему доменских имена. Он обухвата криптографско повезивање Интернет ресурса који је дигитално потписани, затим податке о томе ко потписује тај ресурс, односно име домена и податке о временском периоду у ком је тај потпис валидан. Уколико сервер подржава DNSSEC он ће на захтев клијента покушати да одговори адекватним одговором у виду релевантног записа и одговарајућег потписа. Потпис конкретног записа садржи податке о алгоритму који је коришћен, периоду валидности,

потписнику и дигиталном потпису. Поред података о алгоритмима за дигитално потписивање и за криптографију са јавним кључевима, резервисан је простор за дефинисање разних приватних алгоритама који се могу подешавати локано, што може представљати битан извор безбедности за информационе системе који су реализовани уз подршку Интернета. Обзиром да је име потписника истовремено и име домена, на тај начин се обезбеђује једнозначна идентификација DNS записа и SIG записа.

Кључ, односно KEY (енгл. *Key*) је запис који садржи јавни кључ из пара јавног и приватног кључа и он је генерисан на основу DNS имена домена. Власник кључа (енгл. *The Owner*) може бити DNS зона, клијент који приступа Интернет ресурсима, сервер на ком се физички налазе Интернет ресурси, или неки други ентитет. Запис о Интернет домену, или о неком другом Интернет ресурсу може бити здружен са више различитих записа са дигиталним потписима у зависности од власника кључа. KEY запис садржи кључ, затим алгоритам са којим је кључ третиран, и индекс протокола у зависности од намене кључа. Додатно, овом рекорду се могу налазити и индекси симетричних кључева, односно алгоритама за размену симетричних кључева. Индекс протокола се разликује у зависности од тога да ли се кључеви користе у TLS протоколу (енгл. *Transport Layer Security*), за шифровање електронске поште, DNSSEC – у или IPSec (енгл. *Internet Protocol Security*) протоколу, такође он носи и податак о томе да ли се кључ може користити у свим протоколима. Поред овога, KEY запис располаже резервисаним простором за нове протоколе које је могуће додати у будућности.

DNS има могућност да кешира негативне одговоре. Негативан одговор значи да не постоји запис о Интернет ресурсу који је дефинисан у клијентском захтеву. DNSSEC обезбеђује дигиталне потписе и у случају непостојећег имена (енгл. *Nonexistent Name*), како би одређена зона могла бити аутенификована. NXT (енгл. Nonexistent) запис указује на опсег непостојећег DNS имена, или на записе који су из различитих разлога недоступни за постојеће DNS име. Да би DNS могао да пошаље позитиван одговор, односно да би занемарио неслагање између имена власника и имена Интернет ресурса, DNS користи концепт првог следећег имена. Када клијент пошаље захтев за непостојећим именом, сервер одговара клијенту одговором у виду NXT записа који садржи DNS име првог следећег DNS записа по канонском редоследу. Када недостаје запис за постојеће DNS име, NXT запис садржи DNS име и адекватни потпис који је генерисан на основу дигиталног потписа постојеће зоне.

Дигитални сертификат за сервере, односно CERT (енгл. *Certificate*) је запис који садржи податке о алгоритмима који су коришћени, затим о типовима сертификата и о врсти конкретног сертификата. Додатно, овај запис може садржати податке о алгоритмима који су коришћени приликом генерисања вредности које су смештене у KEY и SIG записе, а који нису предефинисани за употребу у оквиру DNSSEC – а. То омогућава да дигитални сертификат буде креиран уз помоћ алгоритама који нису стандардни за DNSSEC, док су уобичајени типови сертификата дефинисани X.509 стандардом. Један део CERT записа садржи путању до Интернет локације, односно апсолутни URI на којој се може наћи детаљна документација конкретном формату сертификата. Та документација подразумева и листу повучених сертификата, односно CRT (енгл. *Certificate Revocation List*). Безбедност података је разлог за постојање CERT записа. То је важно због тога што се тако омогућава да DNS приступи јавним кључевима разних Интернет ресурса, а да при томе не приступа директно KEY запису, већ да само упоређује вредности након примене криптографских алгоритама на податке који су стигли у оквиру конкретног захтева.

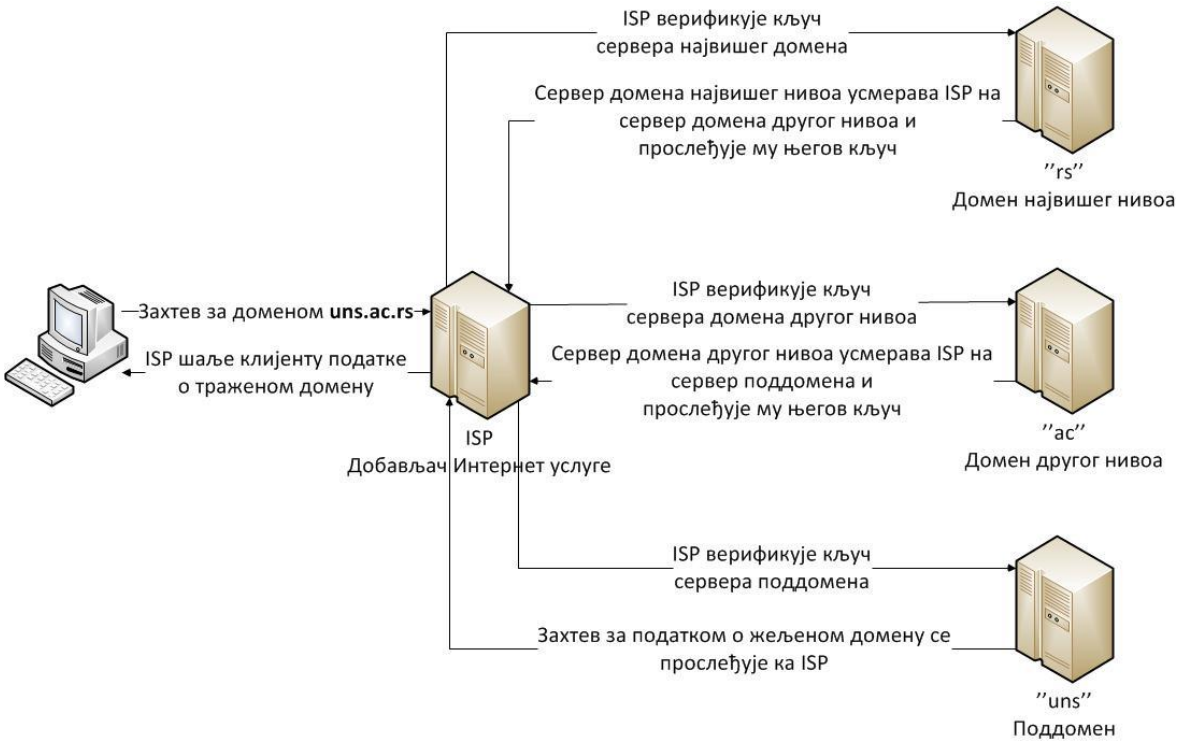
Употреба јавних кључева приликом дигиталног потписивања сервера, односно DNSKEY (енгл. *Domain Name System Public Key*) и употреба низова дигитално потписаних података у сврху делегирања потписа, односно DS (енгл. *Delegation Signer*) омогућава да се докаже да је подређена зона дигитално потписана и тиме се експлицитно дефинише делегација. Ови додаци не шифрују податке и не мењају постојећи систем датотека и директоријума што омогућава потпуну компатибилност са постојећим DNS апликацијама. Они, такође, не утичу на постојећи протокол који је задужен за адресирање већ се на њега надовезују низом дигиталних потписа за сваки ниво у DNS хијерархији, тиме градећи ланац поверења. Приликом провере аутентичности, DNSSEC прати ланац поверења до основног домена (енгл. Root Domain) аутоматски проверавајући сваки подређени домен. Обзиром да је за сваки ниво аутентичност делегирана од стране надређеног нивоа, једина вредност коју је потребно проверити у целом домену јесте аутентичност најнижег домена јер се подразумева аутентичност свих надређених домена.

DNSSEC подразумева дигитално потписивање са две врсте криптографских кључева: дугорочни кључеви за дигитално потписивање краткорочних кључева, односно KSK (енгл. *Key Signing Key*) и краткорочни кључеви за дигитално потписивање DNS записа, односно ZSK (енгл. *Zone Signing Key*). Сви криптографски кључеви се морају мењати у оптималним року како би се спречило њихово компромитовање. Уколико би потенцијални нападач имао довољно времена да примени напад грубе силе и да открију приватни кључ од пара кључева за шифровање, овај систем не би био безбедан. DNSSEC превентивно делује заменом и повлачењем кључева у оптималним временским периодима што смањује могућност за успешан напад. Тај временски период је кратак када су у питању краткорочни кључеви за потписивање зона, најчешће три месеца, а дужи, најчешће годину дана, када су у питању дугорочни кључеви. Обзиром да се са KSK потписују ZSK, а са ZSK потписују DNS записи, једино је KSK потребан како би се проверила аутентичност DNS записа.

3.1 Начин рада DNSSEC сервера

Да би систем доменских имена уз безбедносна проширења био потпуно функционалан потребно је успоставити ланац поверења који полази од основних DNS сервера, root DNS сервера и који се протеже даље дуж стабла свих грана система доменских имена. Да би ово било могуће потребно је да буду дигитално потписани сви сервери на путу од врховног DNS сервера, преко DNS сервера за основне домене, до DNS сервера за доменска имена другог нивоа и поддомена. Примера ради, да би се увео систем дигиталног потписивања DNS сервера за доменско име *tfzr.uns.ac.rs* потребно је да дигитално потписивање буде уведено основни домен *rs*, затим за домен другог нивоа за *ac.rs*, и за његов поддомен *uns.ac.rs*, након чега је могуће дигитално потписивање доменског имена *tfzr.uns.ac.rs*. Специфичност проблематике дигиталног потписивања је и у томе што није могуће реализовати потпуно безбедан систем уз парцијална решења. Поред тога, DNSSEC спецификација претпоставља да DNS сервери подржавају EDNSO (енгл. *Extension mechanisms for DNS*) екстензију која подразумева да UDP пакети (енгл. *User Datagram Protocol*) имају дужину већу од 512 бајтова колика је стандардна дужина UDP пакета, што може узроковати да пакети на неким серверима буду идентификовани као неисправни и као такви одбачени. Такође, дигитално потписивање подразумева временску и просторну синхронизацију ресурса, јер

уколико то није испуњено постоји могућност да провера података буде неуспешна. Због тога је потребно да DNS сервери функционишу у складу са протоколима за усклађивање временских разлика, NTP (енгл. *Network Time Protocol*) и да буду одређени када је у питању њихова физичка позиција помоћу система за глобално позиционирање, GPS (енгл. *Global Positioning System*).



Слика 2 *Креирање ланца поверења*

Дигитално потписивање података DNS – а подразумева потписивање свих компоненти система што обезбеђује да рекурзивни упити и одговори сервера на те упите не буду компромитовани, односно да не буду модификовани и замењени неким лажним подацима, а што је у складу са правилима која су дефинисана у оквиру актуелне спецификације DNSSEC – а. До данас је дигитално потписана врховна зона, односно *root* зона, или „.“ зона, а након ње и већина зона основних домена, првенствено *edu* и *net*, недуго затим и *com*, а након тога већина преосталих, што је створило могућност дигиталног потписивања домена другог нивоа. Управни одбор Фондације "Регистар националног Интернет домена Србије" је у Плану програма и рада за 2014. годину донео одлуку о дигиталном потписивању основног домена *rs*. Регистар националних интернет домена Србије је преузео на себе регистрацију националних интернет домена *pc*, *co.rs*, *org.rs*, *edu.rs*, *in.rs*, као и *срб*, *пр.срб*, *орг.срб*, *обр.срб* и *од.рсб*, док је управљање адресним просторима *ac.rs* и *ak.srb* препуштено Академској мрежи Србије, а *gov.rs* и *upr.srb* Управи за заједничке послове републичких органа. Увођење DNSSEC – а за домаће *rs* и *срб* доменске просторе које је започео Регистар националних интернет домена Србије, према документацији која је тренутно доступна путем Интернета, још увек није реализовано.

Потпуна имплементација DNSSEC - а у домаћи доменски простор би омогућила креирање ланца поверења између свих домаћих доменских имена, а дигитално

потписивање би било централизовано и под контролом домаћих институција, што је значајно обзиром на то да онај који дигитално потписује DNS записе, држи контролу над информацијама. Република Србија треба да заговара потпуну имплементацију DNSSEC – а и требала би да буде и највећи спонзор његовог развоја обзиром на бројне предности које би омогућила реализација овог вида заштите и контроле. Контрола ресурса на Интернету преставља извор моћи и ствара могућност за утицај на даљи развој безбедних Интернет технологија и на обезбеђивање информационе и економске предности у региону. DNSSEC се заснива на изградњи и одржавању ланца поверења, што се у основи своди на безбедност приватних кључева.

3.2 Управљање кључевима у DNSSEC – у

Поступак потписивања Интернет зона подразумева примену криптографије са јавним кључевима и употребу асиметричних алгоритама. Почетни корак је генерисање два криптографска кључа: први за потписивање Интернет зоне, а други за потписивање тог кључа, односно генерисање пара кључева, јавног и тајног за сваки од њих. Софтвер за потписивање је често конципиран тако да корисницима омогућава да изаберу између неколико понуђених алгоритама за креирање отиска поруке. Након креирања парова јавних и тајних кључева, њихове вредности се смештају у одговарајуће датотеке, првенствено у две датотеке од којих једна садржи јавни, а друга тајни кључ, а затим и у датотеку која је везана за конкретну Интернет зону (енгл. *DNSSEC Zone File*) и која, између осталих података садржи и вредности овог пара кључева. Након окончања поступка генерисања кључева, њиховог складиштења, затим и објављивања, може се реализовати дигитално потписивање Интернет зоне. Комплетна Интернет зона се потписује кључем за потписивање зоне, а DNSKEY запис са кључем за потписивање Интернет зоне и кључем за његово потписивање, након чега DNSKEY запис постаје јавни кључ те зоне. Овај поступак резултира креирањем нове датотеке која садржи податке о потписивању комплетне Интернет зоне и која је релевантна у поступку аутентификације. Управљање криптографским кључевима се може реализовати кроз различита решења, а сва се могу окарактерисати двојако: као решења која омогућавају низак ниво безбедности и решења која омогућавају висок ниво безбедности.

Решења са ниским нивоом безбедности се односе на софтверско управљање кључевима са мањим, или већим нивоом аутоматизације. Уколико се ручно управља кључевима то пружа релативно висок ниво безбедности обзиром да кључеви нису постављени од стране компјутера, али људи су склони грешкама, и уколико је потребно мануелно заменити приватне кључеве, извесно је да ће у том поступку временом доћи до грешке, а шанса за то расте повећањем учестаности замене кључева. Значајан аспект управљања кључевима у овом контексту је ограничење приступа читању кључева само на оне људе чији је увид неопходан како би кључеви били замењени. Софтверско генерисање кључева мора да поседује адекватне нивое заштите како би само адекватна апликација из DNSSEC – а имала приступ кључевима, на пример апликација за потписивање зоне. Поред овога, потребно је да само одређене улоге у систему могу да приступе апликацијама за управљање кључевима, обично само врховни администратор. Безбедносни проблем везан за аутоматизацију процеса потписивања се огледа у томе што је потребно да се на серверима за потписивање физички налази кључ за потписивање зона, а како би се умањили негативни ефекти овога, препорука је да сви неауторитативни сервери у ланцу поверења само испоручују потписане зоне при чему их сами не потписују.

Висок ниво безбедности подразумева употребу хардверских решења за руковање кључевима, што је нарочито битно ако се користи динамички DNS и када приватни кључеви треба да буду доступни путем Интернета. Под адекватним хардвером подразумевају се криптографски модули који су отпорни на неовлашћене покушаје приступа, или где није могуће сакрити доказе о неовлашћеном приступу. Они постоје у различитим формама, као мрежни уређаји, као картице и слично, а за све је карактеристично да се генерисање кључева одвија унутар њих и да приватни кључеви никада не напуштају ове модуле у облику отвореног текста, већ искључиво у шифрованом облику. Поред овога, обезбеђивање високог нивоа безбедности подразумева превентивно деловање и онемогућавање потенцијалних нападача да инсталирају злонамерне програме на сервер који би им омогућили да измене DNS податке пре дигиталног потписивања. Због овога, системи који управљају кључевима морају имати безбедне и посебно модификоване оперативне системе на којима раде DNSSEC апликације.

3.3 Аутоматизација процеса у DNSSEC – у

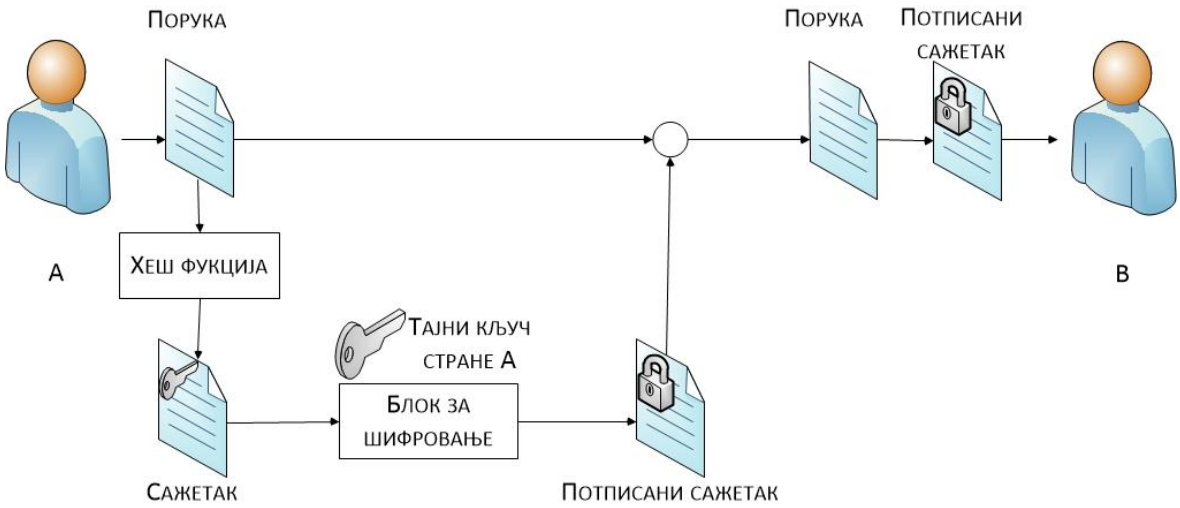
Како би DNSSEC задовољио безбедносне критеријуме потребно је развити систем за управљање криптографским кључевима који би издавао и повлачио кључеве у оптималним временским периодима. Поступак замене кључева пре истека њихове валидности започиње генерисањем новог пара кључева чије вредности се додају у датотеку конкретне Интернет зоне, док се та зона поново потписује текућим, односно старим и још увек важећим кључевима. Овај поступак укључује креирање новог DNSKEY записа на основу новог пара кључева. Подаци о дигиталном потписивању Интернет зоне ће бити доступни свим DNS серверима. Обзиром да подаци којима располажу DNS сервери имају ограничен период важења, односно TTL (енгл. *Time To Live*), ти сервери ће се у предвиђеним временском периоду изменити податке у односу на нове вредности. DNS сервери покушавају да реализују процес аутентификације на основу свих доступних кључева, а успешна аутетификација је могућа обзиром на постојање старих, важећих кључева. Након истека периода важења, обзиром да су сви DNS сервери изменили податке, врши се потписивање Интернет зоне новим кључем. Након истека још једног TTL периода сви DNS сервери имају податак о новом дигиталном потпису Интернет зоне, након чега је могуће повући стари кључ за потписивање те Интернет зоне.

DNSSEC подразумева обављање одређеног броја процеса у оквиру прецизно дефинисаних временских интервала због чега одређени ниво аутоматизације представља решење које умањује шансу да настану грешке. Уколико је процес аутоматизације на нижем нивоу, то подразумева веће ангажовање корисника система, при чему систем обавештава кориснике о потребним акцијама. Како безбедност система не би била угрожена, корисници морају да имају адекватне дозволе за приступ кључевима док сам систем мора да буде конфигурисан тако да за све активности у оквиру система постоји најнижи могући ниво корисничких привилегија уколико, ако дође до људске грешке, или грешке у ради система, не дође до компромитовања кључева. Поред тога, низак ниво аутоматизације захтева да корисници система буду добри познаваоци DNSSEC процеса и да буду спремни да брзо и ефикасно реагују уколико дође до појаве грешака, или до отказивања неког од делова система. Висок ниво аутоматизације омогућава функционисање система уз релативно мало ангажовање корисника, при чему су у систем имплементирани принципи најбоље праксе. Међутим, учешће корисника у неким од процеса може

бити пожељно, на пример слање записа приликом замене кључева за потписивање зона, при чему је потребно ажурирати родитељску зону, такође могуће је аутоматски проверити да ли је процес ажурирања успешно извршен, или и то може бити задатак за неког од корисника. Потреба за познавањем процеса у DNSSEC – у од стране корисника је знатно мања када су у питању системи са вишим нивоима аутоматизације и најчешће ово подразумева да и у случају отказивања система копије потписника зоне могу да преузму контролу над процесом потписивања. Идеална решења не постоје, а конкретна имплементација зависи од практичних захтева које диктира сценарио примене, при чему је неопходно направити компромис између нивоа безбедности и аутоматизације уз то да приоритет треба дати безбедном управљању кључевима, јер на њима почива интегритет домена обезбеђеног уз помоћ DNSSEC – а.

3.4 Дигитално потписивање у DNSSEC – у

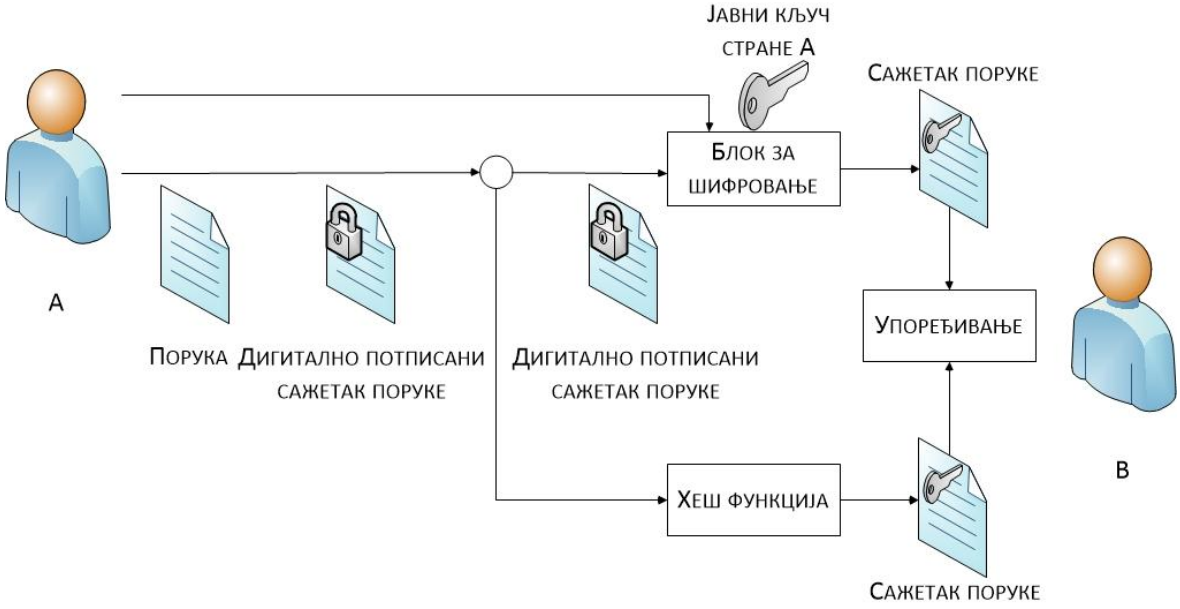
Дигитално потписивање података у оквиру безбедносних проширења за систем доменских имена се реализује у складу са стандардима који су описани у оквиру RFC (енгл. *Request for Comments*) докумената које издаје IETF (енгл. *Internet Engineering Task Force).* Ови стандарди претпостављају да систем мора подржавати потписивање уз употребу RSA/SHA-1 алгоритама, односно уз употребу RSA/SHA-256 и RSA/SHA-512, RSA (*Rivest, Shamir, Adleman*), SHA (енгл. *Secure Hash Algorithm*) алгоритама, поред чега би требао да подржава потписивање на основу ECDSA P-256/SHA-256 и ECDSA P-384/SHA-384 алгоритама, ECDSA (енгл. *Elliptic Curve Digital Signature Algorithm*). Мора да подржи DS (енгл. *Delegation Signer*) записе објављене са SHA-256 отиском поруке. Систем мора подржавати NSEC и NSEC3 (енгл. *Nonexistence*) записе који омогућавају управљање случајевима када се креирају захтеви за доменска имена које не постоје међу записима доменских имена. Систем потписивања би требао да подржава паралелно потписивање са два, или више алгоритама, такође, требао би да омогући преласке између алгоритама за потписивање и промену параметара NSEC и NSEC3 записа без довођења зоне у непотписано стање. Поред тога, систем мора омогућити конфигурисање периода важења потписа.



Слика 3 *Дигитално потписивање*

3.5 Валидација дигиталних потписа у DNSSEC – у

Валидација дигиталног потписа, у складу са стандардима и у складу са избором алгоритма за потписивање мора подржавати алгоритме, RSA/SHA-1, као и RSA/SHA-256 и RSA/SHA-512, а требала би да подржава ECDSA P-256/SHA-256 и ECDSA P-384/SHA-384 алгоритме, затим мора подржавати NSEC3 и мора подржавати DS записе објављене са SHA-256 отиском. Систем валидације би требао да подржава аутоматско ажурирање података за упоређивање, односно за аутоматско ажурирање поузданих полазишта и могућност аутоматског искључења поступака валидације за део, или за комплетан именски простор. Кључни фактор у процесу валидације представља TTL вредност која се додељује записима ресурса. Оптимална временска вредност валидности кључева зависи од њихове намене и комплексности. Велике TTL вредности могу довести до проблема приликом замене кључева, такође могу значајно повећати време опоравка у случају кварова у систему, са друге стране, мале TTL вредности омогућавају већу флексибилност система, али додатно оптерећују серверске и мрежне ресурсе. Пракса је показала да највећи део софтверских решења претпоставља додељивање TTL вредности такве да валидност DNS записа потписаних јавним кључем буде три четвртине времена у ком ће бити валидан тај јавни кључ.



Слика 4 *Валидација дигиталних потписа*

4. Закључак

DNSSEC је логичан наставак развоја DNS – а обзиром на безбедносне ризике који су везани за његову експлоатацију, првенствено када је у питању напад на DNS кеш и на лажирање података о симболичким и логичким адресама ресурса на Интернету. Овакви напади омогућавају крађу тајних података корисника, на основу којих је могуће извршити неку превару. Посредством Интернета се може приступити великом броју ресурса који нису интересантни потенцијалним нападачима због којих би било нерационално ангажовати значајне хардверске и софтверске ресурсе са циљем имплементације DNSSEC – а, међутим развој савремених информационо комуникационих технологија је омогућио његову потпуну имплементацију без већих препрека и знатних финансијских улагања. Виши ниво безбедности и могућност контроле су неки од основних разлога за дигитално потписивање ресурса на Интернету, нарочито када су у питању системи за које постоји изражена потреба за потврдом аутентичности, где имплементација DNSSEC – а представља оптимално решење.

Обзиром на сигурност коју пружају безбедносна проширења, већи део домена највишег нивоа је дигитално потписан. Овим је омогућено успостављање ланца поверења, а даља реализација зависи имплементације ове екстензије на DNS сервере на нижим нивоима. Према извештају од 26. фебруара 2017. године, од укупно 1530 домена највишег нивоа, дигитално је потписано 1385, док је о 1375 већ објављен DS запис. Нажалост, *rs* домен још увек није дигитално потписан што представља безбедносни ризик и отвара могућност за различите злоупотребе јер представља алат за посредне и непосредне нападе. Обзиром на извештаје о раду Управног одбора РНИДС имплементација DNSSEC – а је до сада требала да буде успешно реализована, међутим, иако то није случај о разлозима неиспуњења зацртаних циљева нема званичних извештаја. Повећани трошкови везани за имплементацију DNSSEC – а, укључујући трошкове имплементације и обуке запослених за његову употребу, нису непремостива препрека када се узму у обзир предности које омогућава виши ниво безбедности.

Већа комплексност система усложњава организационе и оперативне задатке што повећава и могућност да дође до проблема у раду. Поред тога, имплементацију безбедносних проширења прати и значајно увећање процесирања података и количине саобраћаја па свака грешка, или пад неког од делова система подразумева потребу за ангажовањем значајних ресурса, хардверских и софтверских, укључујући и ангажовање администратора система, јер је неопходно обезбедити континуирано функционисање система. Велика количина података и велики број аритметичко логичких операција везаних за криптографске алгоритме, додатно појачавају ефекте DoS напада који су посебно заступљени када су у питању DNS сервери обзиром да је уз њихову помоћ могуће извести појачане нападе ове врсте и онемогућити нормално функционисање већег броја Интернет апликација истовремено уз значајно већи интензитет негативних ефеката овог напада. Обзирам да не постоји трајна одбрана од DoS напада превенција се своди на имплементацију мрежне инфраструктуре која је у могућности да поднесе овакве нападе без значајног пада перформанси уз увођење ограничења броја упита у дефинисаним јединицама времена.

Литература

1. **A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)** https://www.ietf.org/rfc/rfc1996.txt

2. **Dynamic Host Configuration Protocol** https://www.ietf.org/rfc/rfc2131.txt

3. **Dan Kaminsky** https://en.wikipedia.org/wiki/Dan_Kaminsky

4. Универзитет „Сингидунум“, **Безбедносна проширења DNS-а - (DNSSEC)**, Студија за потребе Регистра националног Интернет домена Србије, Београд, 2014. године.

5. Мр Н. Крајновић, дипл. инж., **Студија оперативног рада DNS сервиса**, Препоруке за оптимално конфигурисање са освртом на Интернет безбедност, Универзитет у Београду, Електротехнички факултет, Београд, 2015. године.

6. Фондација „Регистар националног интернет домена Србије“, **ПЛАН И ПРОГРАМ РАДА УПРАВНОГ ОДБОРА**, Београд 2013. године.

7. Регистар националних Интернет домена Србије, **КВАРТАЛНИ ИЗВЕШТАЈ О РАДУ УПРАВНОГ ОДБОРА РНИДС**, Београд, 2015. године.

8. **DNS Security Introduction and Requirements** https://www.ietf.org/rfc/rfc4033.txt

9. **Resource Records for the DNS Security Extensions** https://www.ietf.org/rfc/rfc4034.txt

10. **Protocol Modifications for the DNS Security Extensions** https://www.ietf.org/rfc/rfc4035.txt

11. **Extension Mechanisms for DNS (EDNS(0))** https://tools.ietf.org/html/rfc6891

12. **TLD DNSSEC Report (2017-02-26 00:02:12)** http://stats.research.icann.org/dns/tld_report/