DOI: 10.19279/TVZ.PD.2017-5-1-08

ANALIZA NAPADA USKRAĆIVANJEM USLUGE U STVARNOM OKRUŽENJU

DENIAL OF SERVICE ATTACK ANALYSIS IN REAL ENVIROMENT

Igor Džanko[1], Ivica Dodig[2], Davor Cafuta[2], Renata Kovačević[2], Tin Kramberger[2]

[1]Tehničko veleučilište u Zagrebu, Zagreb, Hrvatska, Student
[2]Tehničko veleučilište u Zagrebu, Zagreb, Hrvatska

Sažetak

U posljednje vrijeme Internet se značajno unaprijedio i uvelike poboljšao komunikaciju i poslovanje. Više poslovne korisnosti proporcionalno utječe na količinu sigurnosnih prijetnji. Najčešće sigurnosne prijetnje na Internetu čine mrežni napadi. Najčešći mrežni napad zasniva se na onemogućavanju normalne komunikacije. Mrežni napadi koji su usredotočeni na onemogućavanje komunikacije nazivamo Napadima sa uskraćivanjem usluge (engl. Denial of Service – DoS). DoS napad sprječava pristup korisnicima da komuniciraju u okviru napadnute računalne mreže ili onemogućavaju poslužitelja da poslužuju normalne usluge. Različiti mehanizmi su razvijeni za rano otkrivanje i prevenciju od DoS napada na različitim razinama mrežne infrastrukture. Postoji konstantan napor za izradu novog boljeg modela za komunikaciju. Međutim, metode napada također se razvijaju. Kako bi se spriječilo blokiranje evoluirao je novi oblik napada – Distribuirani napadi s uskraćivanjem usluga (engl. Distributed Denial of service napada (DDoS)). Kod DDoS-a napadači su raspoređeni na cijelom Internetu. Koristeći mrežu kompromitiranih računala (engl. Botnet) napad može biti pokrenut istovremeno sa stotina tisuća kompromitiranih računala. Iskorištavajući veliku mrežu kompromitiranih računala izvor napada može biti dodatno skriven korištenjem Distribuiranog reflektivnog napada s uskraćivanjem usluga (engl. Distributive Reflective Denial of Service (DRDoS)).
U ovom radu ćemo predstaviti različite verzije DoS napada.
U pravom mrežnom okruženju, mjerenjem se pokazuje značajnost utjecaja na rad mreže kroz dostupnost poslužitelja. Dodatno, predložiti će se mogućnosti otkrivanja i prevencije takvih napada.

Ključne riječi: *DDoS, Bloomov filtar, SYN/ACK*

Abstract

Lately, the Internet has significantly improved and greatly enhanced communication and business. More commercial usefulness proportionally affects the amount of security threats. The most common security threats on the Internet are network attacks. The most common network attack is based on disabling normal communication. Network attacks that focus on disabling communication are called Denial of Service (DoS) attacks. A DoS attack prevents access to users to communicate within the attacked computer network, or prevent the server to provide normal services. Various mechanisms have been developed for the early detection and prevention of DoS attacks on different levels of the network infrastructure. There is a constant effort to create a new and better model for communication. However, methods of attack are also being developed. In order to prevent blocking, a new form of attack has evolved – Distributed Denial of Service (DDoS) attacks. In a DDoS attack, the attackers are distributed throughout the Internet. By using a malicious distributed computer network (botnet) an attack can be launched simultaneously by thousands of compromised computers (bots). Using a large network of infected computers, an attack source can be additionally hidden by using

Distributive Reflective DoS (DRDoS) attacks. In this paper, we will present the different versions of DoS attacks. In a real network environment, measurements show the significance of the impact on the operation of the network through server availability. Additionally, the possibilities of how to detect and prevent such attacks will be proposed and their usefulness is discussed.

Keywords: *DDoS, Bloom filter, SYN/ACK*

1. Uvod

1. *Intoroduction*

Razvojem Interneta, osobnih računala i računalnih mreža raste mogućnost sigurnosnih prijetnji, ranjivosti i štetnih napada. Hakeri, virusi, osvetoljubivi zaposlenici i čak ljudska pogreška neke su od opasnosti na mreži. Internet je nedvojbeno postao najveća mreža javnih podataka, uključujući i olakšanu osobnu i poslovnu komunikaciju. Količina prometa koji se prenosi putem Interneta i velikih poslovnih mreža raste eksponencijalno svaki dan. Najveći dio komunikacije zauzima elektronička pošta i poslovne transakcije koje se izvršavaju putem Interneta bilo da zaposlenici na terenu koriste neki oblik preglednika ili udaljeni ogranci velikih tvrtki koriste udaljeno spajanje na mrežu tvrtke da bi izvršili svoje zadatke.

Internet je transformirao i uvelike unaprijedio način na koji se obavlja posao, ali je ujedno ta mreža i njoj pripadajuće tehnologije stvorila rastući broj sigurnosnih prijetnji od kojih se tvrtke moraju zaštititi. Mrežni napadi koji najčešće dolaze iz javne mreže interneta su po svojoj prilici puno ozbiljniji kada nanesu štetu tvrtkama koje pohranjuju osjetljive podatke kao što su osobni, medicinski ili financijski zapisi. Posljedice takvih napada mogu načiniti blagu štetu ili kompletno oslabiti mrežu i podatke te tvrtke na način da važni podaci mogu biti izgubljeni, privatnost može biti narušena ili da na dulje vremensko razdoblje mreža bude srušena i neupotrebljiva za korištenje. Zbog svega toga tvrtke moraju imati dovoljno dobru sigurnosnu politiku kako bi klijentima bila omogućena adekvatna komunikacija te kako bi ih zaštitili od napada.

U nastojanju da zaštite svoje korisnike, tvrtke moraju zaštititi svoje zaposlenike i partnere od sigurnosnih prijetnji. Internet i intranet moraju omogućiti brzu i efektivnu komunikaciju između zaposlenika i partnera. Dakako, komunikacija FTODOi učinkovitost uvelike će ovisiti o posljedicama mrežnih napada. Napad može direktno prouzročiti da zaposlenici neko vrijeme ne mogu izvršavati svoje zadatke i da mreža bude nefunkcionalna dok se ne oporavi od štete nastale napadom ili dok se podaci potrebni za rad ne obnove. Uglavnom, gubitak dragocjenog vremena i podataka može uvelike utjecati na učinkovitost i moral zaposlenika.

Napad na mrežu mogu izvršiti hakeri, na takav način da prouzroče štetu na podacima ili da mrežu učine nedostupnom, nesvjesni zaposlenici ostavljajući mrežu ranjivu nehotice najčešće neznanjem te nezadovoljni zaposlenici. Ono što napadač može napraviti je da pošalje virus u mrežu, podmetne program znan kao trojanski konj, pošalje neograničene količine neželjene pošte ili izvrši razne vrste napada.

Programi znani kao trojanski konj ili trojanci najčešće djeluju kao bezopasna ili korisna programska podrška, kao što su računalne igre, ali oni su zapravo prijetnja. Trojanci mogu obrisati podatke, kopirati poruke na listu adresa elektroničke pošte i otvoriti put za napad na računalo. Trojanac se može donijeti samo ako se kopira u sistem na način da bude, skinut s Interneta, prenesen preko diska ili da je otvoren preko priloga poruke.

Postoji velik broj mrežnih napada koji su dokumentirani i koji su uglavnom klasificirani u tri osnovne kategorije: napadi koji samo izviđaju (engl. reconnaissance attacks), napadi koji onemogućuju pristup (engl. access attacks) i napadi uskraćivanjem usluge (engl. Denial of Service-DoS).

Napadima koji samo izviđaju prikupljaju se važne informacije koje hakeri kasnije koriste za kompromitiranje mreže. Najčešće su to programski alati, kao što su skeneri koji snime mrežne resurse i iskoriste potencijalne slabosti u ciljanoj mreži i aplikacijama. Na primjer dosta programske podrške je napravljeno kako bi mrežnim administratorima omogućilo lakšu

promjenu zaporke ukoliko zaposlenik zaboravi svoju lozinku. Ukoliko zaporka dođe u krive ruke, ona može biti vrlo opasno oružje. Takva programska podrška uvelike olakšava rad administratorima te dolaskom lozinke trećoj osobi može uzrokovati neovlašteno korištenje podataka.

Napadi koji omogućuju pristup provode se nakon što se otkriju ranjivosti u mrežnim prostorima, kao što je autentikacijski servis i različiti servisi kao što su primjerice prijenos podataka, posluživanje Internet stranica i slično. Cilj napadača je pronalazak korisničkog računa elektroničke pošte, pristupa bazi podataka ili drugih povjerljivih informacija.

Napadi s uskraćivanjem usluge sprječavaju pristup dijelovima ili cijelim računalnim sistemima. Oni obično šalju veliku količinu mrežnih podataka na različite uređaje koji su spojeni na mrežu neke tvrtke ili Internet, blokirajući tako protok ispravnog prometa. Štoviše, takav napad može biti utjecajniji kada računalo žrtvu napada velik broj napadača preotetih kompromitiranih računala iz različitih mreža. Takav napad nazivamo raspodijeljenim napadom sa uskraćivanjem usluge (engl. Distributed Denial of Service - DDoS).

U drugom poglavlju opisane su vrste napada uskraćivanjem usluga. Treće poglavlje opisuje ranjivost spojnog protokola. Četvrto poglavlje pokazuje problem prilikom ovakvih napada u stvarnom okruženju kod različitih jačina napada. Radi zaštite od takvih napada u petom poglavlju dan je pregled mjera obrana od napada uskraćivanjem usluge. Mjere obrane dijele se na mjere prevencije, otkrivanja i reakcije na napad.

2. Napadi uskraćivanjem usluge

2. *Denial of Service attacks*

Za analizu napada potrebno je razumijevanje mrežnog prometa te njegove kompozicije. Najčešće korištene riječi koje opisuju mrežni promet jesu tok i format. Tok je kratka referenca za mrežni protokol i za poruke koje putuju do svojih odredišta. Format se odnosi na strukturu podataka, okvira, paketa i segmenata. Danas se u mrežnom prometu najčešće koristi spojni protokol (engl. Transport Control Protocol- TCP).

Danas većina mreža radi sa logičkim adresama prema Internet protokolu verzije 4 (engl. IPv4 address). Logička adresa prema raspodjeli mrežnih slojeva spada u treći mrežni sloj. Na trećem OSI sloju podatke sa pripadajućim zaglavljem nazivamo paketima.

U današnje vrijeme nije se lako obraniti od neželjenih paketa na internetu. Jedan od velikih problema u današnjim mrežama je napad s uskraćivanjem usluge koji računalne resurse čini neupot-rebljivima za krajnje korisnike. „United States Computer Emergency Readiness Team" identificirao je simptome koje napadi s uskraćivanjem usluge najčešće uključuju: smanjenje mrežnih performansa, neraspoloživost mrežnih stranica, postavljanje dijelova mreže nedostupnim, povećan broj neželjene elektroničke pošte [1].
Napad uskraćivanjem usluge može biti jedan dio većeg napada, primjerice odvlačenje pozorno-sti lokalnih administratora sa ciljem iskorištavanja određene sigurnosne ranjivosti (engl. Exploit). Propu-snost usmjernika između interneta i lokalne mreže uslijed napada može biti smanjena, kompromitira-jući tako ne samo potencijalno napadnuto računalo nego i cijelu mrežu.

Napad s uskraćivanjem usluge može biti izveden na nekoliko načina. Neki od osnovnih oblika napada su [2]:

1. potrošnja računalnih resursa kao što je propusnost, diskovni prostor ili procesorsko vrijeme,
2. prekid konfiguracijskih informacija, kao što su informacije usmjernika,
3. prekid informacija, kao što je nepredviđeno resetiranje spoja ostvarenih spojnim protokolom,
4. prekid fizičkih mrežnih komponenti,
5. ometanje komunikacijskog medija između korisnika i žrtve tako da oni više ne mogu komunicirati.

Slika 1 *Primjer napada uskraćivanjem usluge*

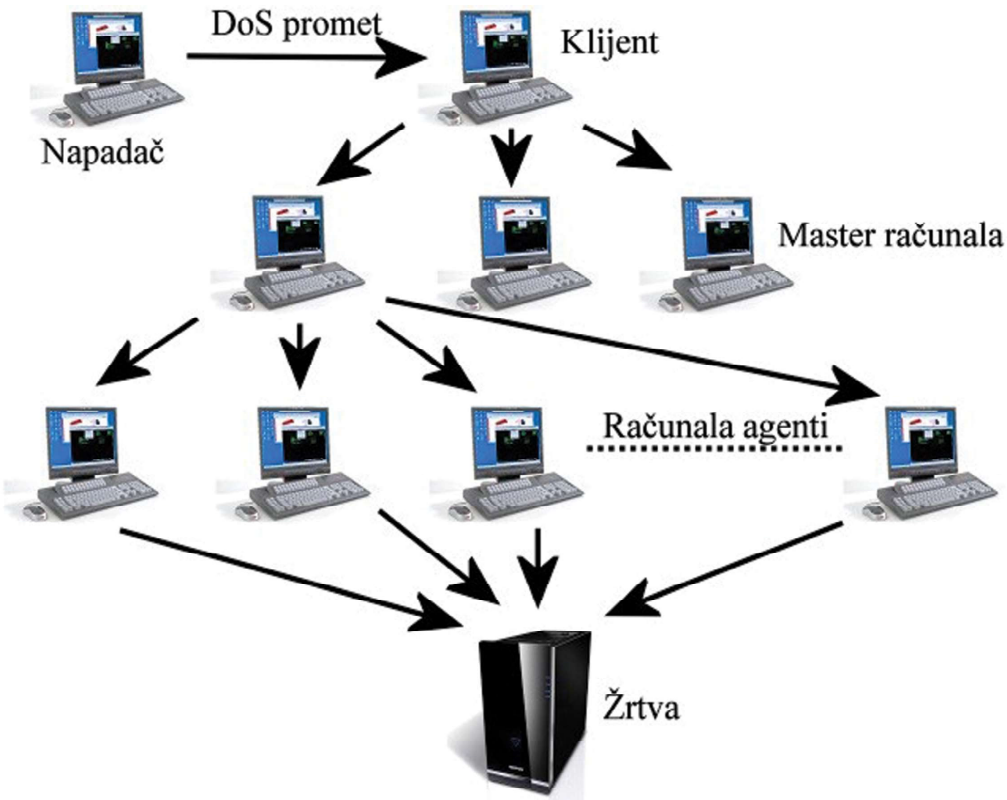
Figure 1 *An example of an attack by denial of service*

Jedan od najjednostavnijih napada s uskraćivanjem usluge, s obzirom na broj posrednika između napadača i žrtve, prikazan je na slici 1. U ovom slučaju napadač putem Interneta šalje neželjene pakete ne koristeći nikakve posrednike između njega i ciljanog poslužitelja nad kojim izvršava napad

Ukoliko se dogodi da između napadača i žrtve postoji niz posrednika, napad prelazi u raspodijeljeni napad uskraćivanjem usluge. Na ovaj način napadač otežava otkrivanje izvora napada. Primjer provedbe napada prikazan je na slici 2. Napadač napad pokreće preko upute središnjem računalu koje upravlja mrežom kompromitiranih računala (engl. botnet). Središnje računalo distribuira uputu nizu klijenata direktno ili preko dodatnih posredničkih klijenata radi sakrivanja izvora upute. Kompromitirana računala nakon zaprimanja upute u zadano vrijeme pokreću napad uskraćivanjem usluge prema žrtvi. Kako je mreža kompromitiranih računala globalna ona sadrži računala koja su raspodijeljena u mnoštvo različitih autonomnih sustava.

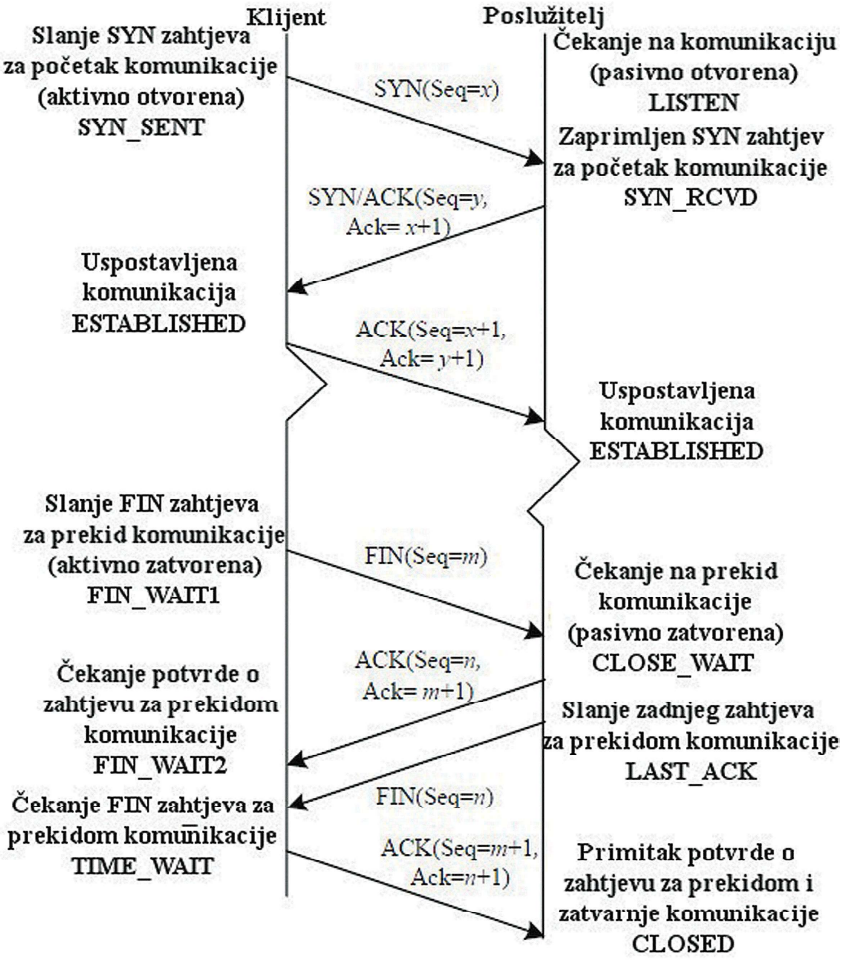
Na ovakav napad žrtva ne može odgovoriti blokiranjem izvora napada budući da kod velikih mreža zlođudnih računala to može iziskivati zabranu velike većine autonomnih sustava na cijelom Internetu. [3].

Ukoliko se u napadu uvede dodatan stupanj tako da računala agenti šalju zahtjeve na računala koja dalje reflektiraju napad prema žrtvi, napad prelazi u raspodijeljeni reflektirani napad uskraćivanjem usluge (engl. Distributed Reflective Denial of Service-DRDoS). Kod ovakvog napada, napadač upravlja posrednicima tako da oni šalju napadački promet do reflektora s podvaljenom IP adresom žrtve, i onda reflektori šalju dalje promet prema žrtvi uzrokujući napad uskraćivanjem usluge. Reflektori su još jedan nivo računala koji povećavaju količinu prometa. Na taj način reflektori omogućuju napadaču da se uvelike oteža pokušaj pronalaska izvorišne mreže iz koje je došao napad [4].



Slika 2 *Primjer raspodjeljenog napada uskraćivanjem usluge*

Figure 2 *An example of a distributed denial of service attack*



Slika 3 *Uobičajena komunikacija kod početka i kraja u spojnom protokolu*

Figure 3 *Common communication at the beginning and end of the connection protocol*

3. Ranjivost spojnog protokola

3. *Connection protocol vulnerability*

Prema sigurnosnim izvještajima napad uskraćivanjem usluge slovi kao jedna od glavnih prijetnji na Internetu. Većina njih iskorištava ranjivosti spojnog protokola na transportnom sloju. Najveći udio podvrste napad uskraćivanjem usluge čini napad slanjem prekomjernog broja sinkronizacijskih paketa (engl. SYN Flood) [5][6].

Napad slanjem prekomjernog broja sinkronizacijskih paketa iskorištava ranjivost spojnog protokola. Spojni protokol se uspostavlja u 3 stupnja gdje klijent i poslužitelj izmjenjuju poruke za uspostavljanje konekcije (slika 3).

Komunikacija počinje tako da klijent poslužitelju šalje paket zahtjeva spoja (SYN).

Kada poslužitelj primi paket zahtjeva spoja, on rezervira neke od potrebnih resursa za očekivani spoj i šalje klijentu potvrdu primitka zahtjeva spoja (SYN/ACK). Klijent potvrđuje primitak potvrde zahtjeva spoja (ACK), te se time spoj uspostavlja. Po primitku paketa poslužitelj i klijent mogu početi izmjenjivati podatke. Svaka skupina podataka koja se šalje (engl. Window) mora biti potvrđena paketom potvrde podataka. To čini ovaj protokol pouzdanim budući da se može ustanoviti gubitak i zatražiti ponovni prijem informacije. Nakon obavljene komunikacije jedna strana započinje proces prekida veze slanjem zahtjeva za prekid komunikacije (FIN). Druga strana potvrđuje paketom potvrde zahtjeva za prekid komunikacije (ACK), te dodatno šalje paket zahtjeva za prekid komunikacije u drugom smjeru (FIN). Temeljem toga zahtjeva dodatno se odgovara paketom potvrde prekida spoja (ACK).

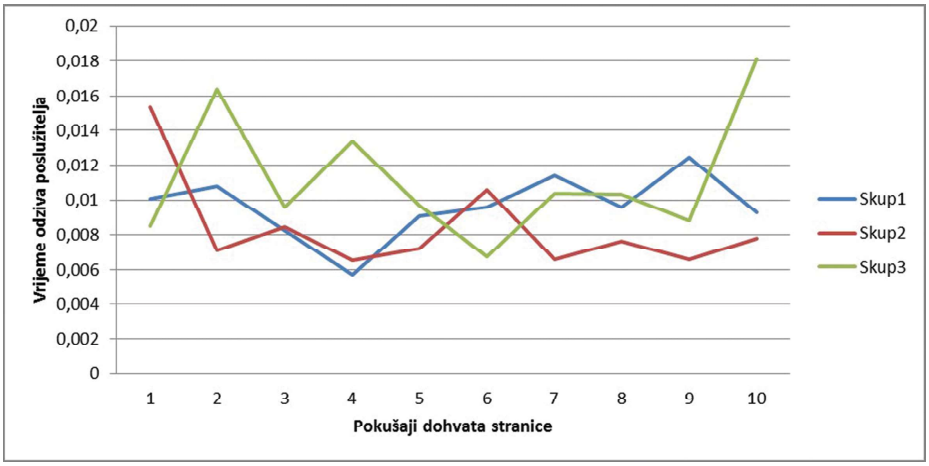
Nakon prijema potvrde toga zahtjeva spoj se prekida. Napad prekomjernim slanjem sinkronizacijskih paketa izvodi se tako da klijent nikada ne pošalje paket potvrde spoja.

Obzirom na očekivanu uspostavu spoja poslužitelj rezervira potrebne resurse i očekuje potvrdu. Rezervirani resursi poslužitelja na poluotvorenom spoju oslobađaju se tek nakon određenog vremena (engl. TCP timeout). Budući da su sistemski resursi konačni i ograničeni, on uskoro neće moći primati nove zahtjeve za ostvarenje spoja.

4. Analiza napada u stvarnom okruženju
4. *Attack analysis in real surroundings*

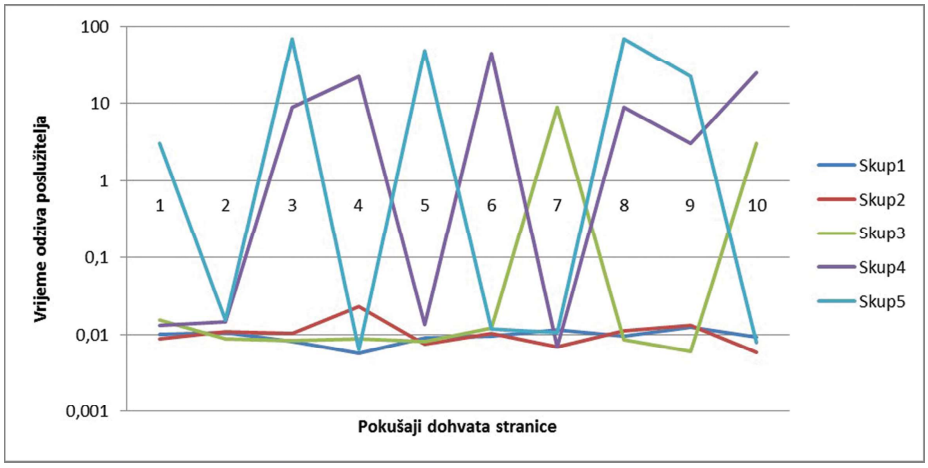
Temeljem opisa spojnog protokola ovakva vrsta napada moguća je na postojećoj mrežnoj arhitekturi verzije četiri (IPv4), kao i na nadolazećoj mrežnoj arhitekturi verzije šest (IPv6) [7]. U svrhu potvrde ove teze provedena je analiza utjecaja napada prekomjernim slanjem sinkronizacijskih paketa na poslužitelj Internet stranica. U analizi računalo napadač slalo je poruke različitim intenzitetima prema mrežnoj kartici žrtve. Koristeći treće računalo mjerena je brzina odziva Internet stranice sa poslužitelja žrtve. Radi eliminacije utjecaja mreže računalo koje mjeri spajalo se na mrežnu kartice žrtve koja je bila u zasebnoj mreži u odnosu na karticu na koju je vršen napad. Testiranje je provedeno na staroj i na novoj verziji protokola mrežnih adresa (IPv6). Grafovi na slikama 4a i 4b i 4c prikazuju brzinu dohvata Internet stranica koja je u ovisnosti o intenzitetu napada na drugoj mreži. Horizontalna koordinatna os sadrži pokušaje pristupa internet stranici poslužitelja žrtve, a vertikalna os prikazuje brzinu odziva poslužitelja u sekundama. Na slikama 4b i 4c je vertikalna os u logaritamskoj skali. Podaci pod nazivom skup1 na slikama 4a i 4b prikazuju odziv poslužitelja dok nema napada. Na slici 4a prikazan je skup podataka pod nazivom skup2 kod kojeg se napad izvršavao slanjem samo jednog paketa u sekundi, dok podaci pod nazivom skup3 prikazuju odziv kod napada koji je generiran slanjem paketa svake 0,2s. Iz grafa sa slike 4a uviđa se problem otkrivanja napada manjeg intenziteta.
Slika 4b prikazuje odzive kod jačeg intenziteta napada gdje su se napadi izvršavali slanjem paketa svakih: 0,09s za skup2, 0,07s za skup3, 0,05s za skup4 i 0,03s za skup5. Radi jasnijeg prikaza dobivenih podataka na slici 4c prikazane su krivulje za minimalne, prosječne i maksimalne vrijednosti vremena za pojedini intenzitet napada za podatke uzete sa slike 4b. Skup1 ovdje prikazuje minimalne vrijednosti kod pojedinih dohvata stranice, skup2 prosječne vrijednosti i skup3 maksimalne vrijednosti za dohvat stranice sa poslužitelja. U tabeli 1 su vrijednosti za koje je prikazan graf na slici 4a. Tabela 2 ima vrijednosti koje prikazuju graf na slici 4b, kao i njihove minimalne, prosječne i maksimalne vrijednosti prikazane grafom na slici 4c.

Uzevši u obzir dobivene rezultate dolazi se do spoznaje da je moguće izvesti napad prekomjernim slanjem sinkronizacijskih paketa unutar lokalne mreže samo sa jednim računalom napadačem. Obzirom na sličnost dobivenih rezultata u mrežnoj arhitekturi verzije četiri i verzije šest na slici je prikazano ponašanje mrežne arhitekture verzije šest.



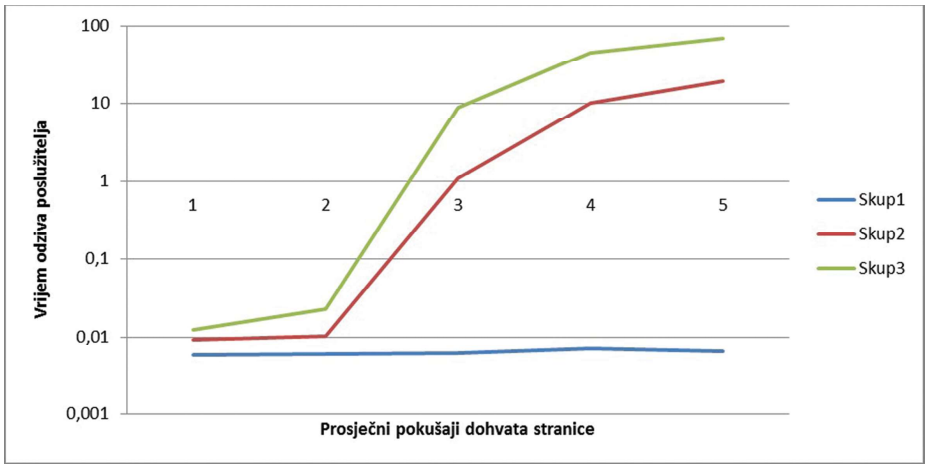
Slika 4a *Prikaz odziva poslužitelja za različite intezitete napada*

Figure 4a *Depiction of the server response for different intensities of attack*



Slika 4b *Prikaz odziva poslužitelja za različite intezitete napada*

Figure 4b *Depiction of the server response time for different intensities of the attack*



Slika 4c *Prikaz prosječnog odziva poslužitelja za različite intezitete napada*

Figure 4c *Depiction of the server's average response time for different intensities of attack*

Tabela 1 *Vrijednosti uz graf na slici 4a*

Table 1 *Values for the graph in figure 4a*

	JAČINA NAPADA		
POKUŠAJI	**BEZ**	**1**	**0,2**
1.	0,010049	0,015359	0,008493
2.	0,01079	0,007099	0,016355
3.	0,008234	0,008433	0,009582
4.	0,00573	0,006522	0,013365
5.	0,00905	0,007218	0,009707
6.	0,009581	0,010579	0,006745
7.	0,011405	0,006578	0,010387
8.	0,00959	0,007633	0,010292
9.	0,012465	0,006595	0,008792
10.	0,009305	0,007777	0,018141

Tabela 2 *Vrijednosti uz grafove na slikama 4b i 4c*

Table 2 *Values for the graph in figures 4b and 4c*

	JAČINA NAPADA				
POKUŠAJI	**BEZ**	**0,09**	**0,07**	**0,05**	**0,03**
1.	0,010049	0,008721	0,015509	0,013183	2,999246
2.	0,01079	0,010995	0,008772	0,014598	0,015375
3.	0,008234	0,010351	0,008369	9,011754	68,99973
4.	0,00573	0,023027	0,008744	22,01041	0,006453
5.	0,00905	0,007404	0,008125	0,013452	48,0132
6.	0,009581	0,010391	0,012227	45,00672	0,011848
7.	0,011405	0,007008	9,005233	0,006844	0,010619
8.	0,00959	0,01118	0,008659	9,002233	69,0095
9.	0,012465	0,013093	0,006025	3,000195	22,00788
10.	0,009305	0,00589	3,00529	25,00948	0,007942
MINIMUM	0,00573	0,00589	0,006025	0,006844	0,006453
PROSJEČNO	0,009266	0,010359	1,099362	10,28143	19,18984
MAKSIMUM	0,012465	0,023027	9,005233	45,00672	69,0095

5. Mjere obrane od napada uskraćivanjem usluge

5. *Measures of protection from denial of service attacks*

Nagli razvoj Interneta u poslovne svrhe utjecao je značajno i na sigurnost računalnih mreža, što je dovelo i do pojave sigurnosnih prijetnji. Neki od primjera prijetnji su napadi uskraćivanjem usluge, upadi na mreže, napadi lažnim identitetom i generiranje neželjene pošte. Većina aktualnih prijetnji se povezuje uz napade uskraćivanjem usluge za koji postoje mnoga istraživanja u vidu preventive, otkrivanja i reakcije na napad. Primjeri velikih napada su: Visa, PayPal i Master Card (2010.), Sony Playstation (2011) i napad na Wall Street Exchange Market (2011), što ukazuje na trend daljnjeg povećanja takvih napada [5][6]. Za zaštitu od napada uskraćivanjem usluge mogu se provesti adekvatne mjere u vidu preventive, otkrivanja i reakcije na napad. Preventivnom mjerom se nastoji spriječiti napad iz vlastite mreže filtriranjem. Filtriranje se provodi na ulasku i izlasku iz vlastite mreže. U analizi se odbacuju paketi za koje se ustanovi da žele pristupiti globalnoj mreži sa privatnim ili lokalnim adresama. Obzirom da napad uskraćivanjem usluge često provode kompromitirana računala administrator lokalne mreže na ovaj način sprječava napad u samom izvoru. Uz uvjet da većina lokalnih administratora postavi ovakav sustav mogu se lako spriječiti raspodijeljeni i reflektirani raspodijeljeni napadi uskraćivanjem usluge.

U svrhu otkrivanja razvijeni su algoritmi [8] koji nastoje otkriti napad u stvarnom vremenu. Obzirom da je zahtjevno analizirati promet u stvarnom vremenu primjenjuje se analiza vremenskih isječaka te se time smatra da je dobivena odluka ispravna za cijeli promet. TCP protokol koristi trostruko rukovanje za uspostavu veze, te četverostruko za prekid veze. Očekivano je da će u mrežnom prometu bez napada biti otprilike proporcionalan broj paketa za ostvarivanje i prekid veze. Ako dođe do značajnog poremećaja u tom broju može se zaključiti da je u tijeku napad. Važno obilježje ovih algoritama je definicija praga nakon kojega se smatra postojanje napada.

Ovi algoritmi razlikuju se međusobno obzirom na promatrane parove paketa veze koji analiziraju. Također za pohranjivanje informacija o paketima uglavnom koriste strukturu Bloomovog filtra [9] [10][11][12]. koji smanjuje potrebu za količinom potrebne memorije što pogoduje ugradnji u ugrađeni sustav [13].

Mjera otkrivanja pokreće mehanizme koji svojim djelovanjem ublažuju posljedice napada. Ciljevi sustava zaštite od napada su ublažavanje posljedice napada odnosno osiguranje dostupnost sustava, te određivanje što točnijeg izvora napada. Osim navedenih sustava moguće je postaviti i lažne poslužitelje pomoću kojih se pri izvršenju napada jednostavnije određuje izvor i opseg napada.

6. Zaključak

6. *Conclusion*

Uloga Interneta i drugih mrežnih okruženja danas dobiva sve veći značaj kroz povećanje broja korisnika u poslovnim pa i privatnim okruženjima. Povećanjem broja mrežnih priključaka raste i broj mrežnih spojeva, a time i negativnih sastavnica globalnog okruženja.Napadi uskraćivanjem usluga čine jednu od najvećih prijetnji. Unutar skupine tih napada najčešći su napadi na transportnom sloju. Napad prekomjernim slanjem sinkronizacijskih paketa sa lažiranom izvorišnom mrežnom adresom obuhvaća većinu takvih napada. Otkrivanje napada poželjno je ostvariti kod same pojave napada kako bi se što prije uključile mjere reakcije. Cilj je prepoznati napad što bliže njegovom izvoru. Kod raspodijeljenog napada s uskraćivanjem usluge smisao blokiranja jednoga izvora ne donosi učinkovito rješenje sprječavanja napada. Iz toga razloga idealno mjesto za otkrivanje je na strani žrtve, odnosno na usmjerniku pružatelja internetskih usluga na koji je spojena žrtva napada.
Koristeći omjere SYN/ACK-ACK paketa koji su osnovni elementi svake spojne veze moguće je utvrditi anomalije u mreži. Anomalije potvrđene iznad neke utvrđene granice jasno određuju postojanje napada. Za ispravno otkrivanje potrebno je jasno povezati pripadni SYN/ACK sa ACK paketom. Čuvanje potpunih informacija zaglavlja parova tih paketa traži značajne količine memorije naročito na brzim linkovima u trenutku zagušenja mreže napadom. U tu svrhu parovi paketa organizirani su u memorijsku efikasniju podatkovnu strukturu Bloomov filtar. Koristeći vremenske periode za otkrivanje napada sprječavamo utjecaj podataka u prošlosti i donosimo odluku o postojanju napada koje pokreću mjere reakcije. Implementacija ovakvog rješenja zahtjeva manje resursa (memorije i procesorske snage) čime je pogodna za implementaciju u ugrađeni računalni sustav. Također rezultati su pokazali da se korištenjem strukture dvostrukog Bloomovog filtra smanjuju pogreške prilikom prepoznavanja pripadnih ACK paketa, a da se pri tome neznatno uvećava potreba za memorijskim prostorom.

7. Reference

7. *References*

[1] Mindi McDowell, National Cyber Alert System, URL:http://www.us-cert.gov/cas/tips/ST04015.html , 2007.

[2] Department of Homeland Security: Cyber Security Procurement, Language for Control Systems, URL:http://www.us-cert.gov/control_systems/pdf/

[3] Rocky K.C. Chang, Defending against flooding based distributed denial of service attacks : A tutorial, IEEE Communications Magazine, October 2002.

[4] Vern Paxson, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, 2001, URL:http://www.icir.org/vern/papers/reflectors.CCR.01.pdf, 2001.

[5] Cisco 2016 Annual Security Report: URL: http://www.cisco.com/c/m/en_us/offers/sc04/2016-annual-security-report/index.html, 2016.

[6] DDoS Attacks in Q3 2016, Kaspersky Lab Report, URL: https://securelist.com/analysis/quarterly-malware-reports/76464/kaspersky-ddos-intelligence-report-for-q3-2016/, 2016.

[7] Xinyu Yang, Ting ma, Yi Shi,"Typical DoS/DDoS threats under IPv6, Proceedings of International Multi-Conference on computing in the Global information Technology (ICGI'07) March 2007.Page(s):50-55.

[8] Mehdi Ebady Manna and Angela Amphawan, Review of Syn-Flooding Attack Detection Mechanism, International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012, pp 99-117.

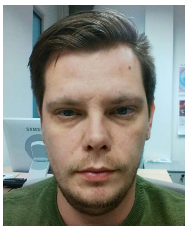
[9] H. Wang, D. Zhang, K.G. Shin, Detecting SYN Flooding Attacks, INFOCOM, IEEE, 2002.

[10] H. Wang, D. Zhang, K.G. Shin, SYN-Dog: sniffing SYN flooding sources, ICDCS, IEEE 2002.
[11] W. Chen, D.Y.Yeung, Defendig against TCP SYN flooding attacks under different types of ip spoofing, 5th International Conference on Networking, 2006.
[12] C. Sun, C. Hu, Y. Tang, B. Liu, More Accuratte and Fast SYN flood detection, IEEE, 2009.
[13] A. Broder, M. Mitzenmacher, Network applications of Bloom filters: Survey, Inernet Mathematics vol1. no.4, 2004

AUTORI · *AUTHORS*

Ivica Dodig
Ivica Dodig je predstojnik Zavoda za računalne mreže i sustave na Informatičko-računarskom odjelu Tehničkog veleučilišta u Zagrebu. Završio je Tehničku školu u Kutini kao Tehničar za elektrostrojarstvo. Po završetku tehničke škole završava Fakultet elektrotehnike i računarstva i stječe titulu diplomiranog inženjera računarstva. Trenutno je doktorskom studiju Fakulteta elektrotehnike i računarstva. Nakon uspješno obavljenog javnog razgovora u pripremi je izrade doktorata. U svom radu stekao je zvanje višeg predavača. Područja interesa su mu otvoreni operacijski sustavi.

Korespodencija
ivica.dodig@tvz.hr



Tin Kramberger
Tin Kramberger rođen je 1983. godine u Zagrebu. Završio je III. gimnaziju u Zagrebu. 2007. godine završava preddiplomski stručni studij informatike na Tehničkom veleučilištu u Zagrebu, nakon čega upisuje specijalistički diplomski stručni studij koji završava 2010. godine. Za cijelo vrijeme trajanja studija radi kao razvojni inženjer. Trenutno radi kao predavač na Informatičko-računarskom odjelu Tehničkog veleučilišta u Zagrebu. Područja interesa su mu baze podataka, umjetna inteligencija i razvoj mobilnih aplikacija.

Korespodencija
tin.kramberger@tvz.hr

Davor Cafuta
Davor Cafuta je voditelj redovnog dodiplomskog stručnog studija računarstva na Tehničkom veleučilištu u Zagrebu. Završio je Tehničku školu Ruđera Boškovića u Zagrebu kao Tehničar za elektroniku. Po završetku tehničke škole završava Fakultet elektrotehnike i računarstva i stječe titulu diplomiranog inženjera računarstva. Trenutno je doktorskom studiju Fakulteta elektrotehnike i računarstva. Nakon uspješno obavljenog javnog razgovora u pripremi je izrade doktorata. U svom radu stekao je zvanje višeg predavača. Područja interesa su mu ugrađeni sustavi i otvoreni operacijski sustavi.

Korespodencija
davor.cafuta@tvz.hr

Renata Kovačević
Renata Kovačević je asistent na Informatičko-računarskom odjelu Tehničkog veleučilišta u Zagrebu. 2012. godine završava preddiplomski stručni studij informatike na Tehničkom veleučilištu u Zagrebu, nakon čega upisuje specijalistički diplomski stručni studij koji završava 2015. godine. Po završetku stječe stručni naziv stručni specijalist inženjer informacijskih tehnologija (struč. spec. ing. tech. inf.). 2015. stječe zvanje asistenta te počinje raditi na TVZ-u. Područja interesa su joj razvoj računalnih igara, razvoj web aplikacija i baze podataka.

Korespodencija
renata.kovacevic@tvz.hr

Igor Džanko
Igor Džanko je student treće godine redovnog dodiplomskog stručnog studija informatike na Tehničkom veleučilištu u Zagrebu. U svom dosadašnjem studiranju postigao je izvrsne rezultate naročito u područjima mrežnih tehnologija i otvorenih operacijskih sustava. Područja interesa su mu ugrađeni sustavi i mrežne tehnologije.

Korespodencija
idzanko@tvz.hr