CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Napadi uskraćivanjem usluge

NCERT-PUBDOC-2011-01-321

Nacionalni CERT

Sadržaj

1 Uvod

U zadnjem desetljeću napadi uskraćivanjem usluga postali su popularni kao jednostavno sredstvo nanošenja štete onima koji pružaju bilo koje usluge putem Interneta. Izvođenje ovih napada svodi se na korištenje dostupnih alata i tehnički nije zahtjevno, no štete koje njime nastaju u pojedinim slučajevima mogu biti i veće od šteta u kojima napadač uspije kompromitirati ciljano računalo.

Usprkos sve većem broju sigurnosnih incidenata koji uključuju napad uskraćivanjem usluge veliki broj organizacija, sistem inženjera i korisnika imaju krivu predodžbu o načinu na koji se napadi izvode i mogućoj zaštiti. Ovaj dokument ukratko predstavlja nekoliko najkorištenijih vrsta napada uskraćivanjem usluge. U dokumentu će biti pojašnjena anatomija izvođenja ovih napada, alati koje kriminalci koriste te savjeti za smanjenje rizika i zaštitu.

2 Definicija i vrste napada uskraćivanjem usluga

Napad uskraćivanjem usluge (eng. *denial-of-service attack*, u daljnjem tekstu DoS) je napad na neko računalo u kojem napadač želi resurse ili servise tog računala učiniti nedostupnim za njihove korisnike. Iako se motivi, načini i ciljane mete ovakvih napada mijenjaju, svima im je zajedničko želja da se pristup uslugama onemogući na kraće ili dulje razdoblje. Svaki DoS napad ima tri uključene strane. To su:

- Napadač – osoba koja provodi napad. On želi oštetiti neko ciljano računalo na Internetu.
- Žrtva – računalo koje trpi napad. Rezultat napada je nemogućnost žrtve da isporuči uslugu svojim korisnicima.
- Korisnici – Sve osobe koje na legalan način koriste usluge žrtve. Za vrijeme DoS napada njima je pristup željenim uslugama onemogućen.

Važno je zapamtiti da DoS napadi ne omogućavaju napadaču neovlašteni pristup žrtvi ili krađu podataka s nje. Ukoliko napadač uspješno provede DoS napad i on sam neće moći pristupiti resursima žrtve kao i svi ostali korisnici.

Termin DoS napad najčešće se pojavljuje u kontekstu računalnih mreža i mrežnih tehnologija budući da se takvi napadi najčešće provode putem njih. No, DoS napadi nisu ograničeni samo na računalne mreže. DoS napad moguće je provesti iskorištavanjem neke sigurnosne ranjivosti u softveru na ciljanom računalu. Npr. napadač može namjerno srušiti poslužitelja elektroničke pošte i time onemogućiti korisnicima da šalju i primaju elektroničku poštu. Provođenje takvih napada moguće je zbog loše kvalitete softvera koji pokazuje brojne ranjivosti. Obrana od ovakvih napada pripada u domenu poboljšanja kvalitete programskog koda i redovitog ispravljanja otkrivenih ranjivosti.

Osim problema sa softverom, svako fizičko uništavanje infrastrukture također je oblik DoS napada. Za uspješno provođenje takvog napada napadač mora imati fizički pristup infrastrukturi. Zaštita od njih spada u domenu kontrole fizičke sigurnosti.

Za razliku od DoS napada putem ranjivosti nekog softvera, DoS napadi koji se odvijaju preko mreže ne ovise o kvaliteti softvera koji žrtva koristi. Bez obzira na kvalitetu softvera, DoS napad preko mreže još uvijek može u potpunosti uspjeti. U usporedbi s fizičkim uništavanjem infrastrukture, za DoS napad putem mreže nije potreban fizički pristup žrtvi i oni ne spadaju u domenu kontrole fizičke sigurnosti.

Ostatak ovog dokumenta posvećen je DoS napadima koji se izvode putem računalnih mreža.

3 Utjecaj i razlozi provođenja DoS napada

Jedan od razloga za provođenje DoS napada želja je za nanošenjem štete određenoj žrtvi. Ukoliko žrtva uvelike ovisi o dostupnosti svojih resursa klijentima, DoS napad joj može prouzročiti značajnu financijsku štetu. Kriminalci su otišli daleko u tome smjeru pa su česti slučajevi iznuda i ucjena. Oni započinju DoS napad na određenu organizaciju i traže financijsku naknadu kako bi napad prekinuli. Kako se veliki broj organizacija ne može obraniti od DoS napada većih razmjera, česti su slučajevi u kojima one plate ucjenu.

Osim direktne ucjene zabilježeni su slučajevi u kojima kriminalci iznajmljuju mogućnost provođenja DoS napada na neku organizaciju ili konkretno računalo. Takve usluge mogu se kupiti na crnom tržištu, a kupci ih obično koriste kako bi konkurentske organizacije što više oštetili na vlastitu korist.

DoS napadi često se provode i kao jedna od faza nekog većeg napada koji za cilj ima dobivanje neovlaštenog pristupa žrtvinom računalu. Ako je za provedbu takvog napada potrebno određeni servis učiniti nedostupnim napadač za to može koristiti neke tehnike DoS napada. Jedan primjer takve situacije može biti napad ne neki od kriptografskih protokola u kojem je privremeno potrebno neki kriptografski servis učiniti nedostupnim.

Utjecaj DoS napada nije zanemariv i danas oni predstavljaju veliki rizik brojnim organizacijama i mrežama. Ovu tvrdnju produbljuje činjenica da samo provođenje DoS napada od napadača ne zahtjeva posjedovanje složenih tehničkih znanja i vještina. Uspješnost provođenja DoS napada ovisi samo o snazi napadača. Ukoliko napadač može prikupiti dovoljno veliki broj računala s kojih će pokrenuti napad moći će oštetiti i najveće računalne mreže.

Kao primjer takvog postupanja moguće je istaknuti dva incidenta, jedan iz 2002. godine, drugi iz 2007. godine. U oba incidenta radilo se o provođenju DoS napada na vršne DNS poslužitelje na Internetu. Vršni DNS poslužitelji (eng. *DNS root nameserver*) osnovni su DNS poslužitelji koji sudjeluju u *resolvingu* TLD domena. Trenutno ima 13 takvih poslužitelja i oni su jedan od osnovnih servisa na Internetu, bez njihova postojanja normalno korištenje Interneta bilo bi gotovo nemoguće. Iako su ovi poslužitelji izgrađeni tako da očekuju velike količine mrežnog prometa, oba navedena incidenta su neke od njih uspjela učiniti nedostupnima. U DoS napadu od 2002. godine čak 9 od 13 DNS poslužitelja bilo je nedostupno, a u incidentu iz 2007. godine, dva poslužitelja su bila nedostupna.

Ovakvi događaji samo svjedoče o tome da pažljivo pripremljen DoS napad može biti opasan ne samo za jednog korisnika ili organizaciju, već za cijeli javni Internet.

4 Vrste napada uskraćivanjem usluge

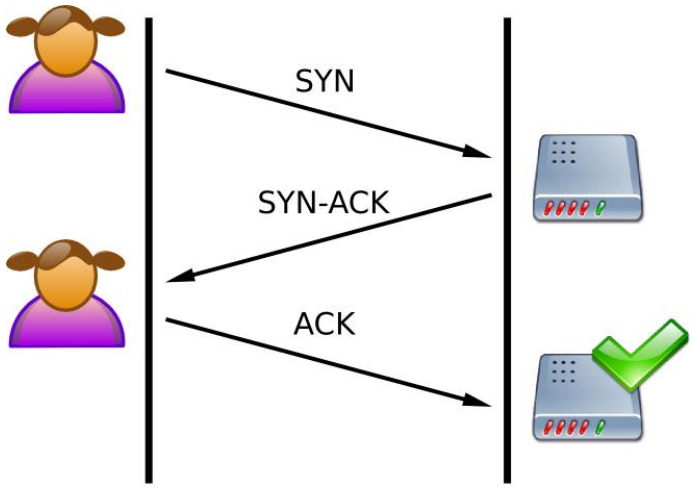
Kao što je već navedeno ovaj dokument posvećen je DoS napadima koji se izvode putem računalne mreže. Kod takvih DoS napada žrtva dobiva veliki broj zahtjeva za uspostavljanjem komunikacije. Kako žrtva ne može obraditi svaki dobiveni zahtjev, a isto tako ne može razlikovati legitimne od zlonamjernih zahtjeva nužno je da neki od tih legitimnih zahtjeva budu odbijeni. Time je žrtva postala nedostupna za svoje legitimne korisnike. DoS napadi putem mreže izrabljuju mogućnosti protokola koji se koriste u komunikaciji kako bi poslali veliki broj zahtjeva žrtvi.

Postoji mnoštvo različitih vrsta napada koji se mogu provesti putem mreže. Različite vrste imaju različit tehnički pristup provođenju napada, ali uvijek isti cilj – učiniti žrtvu nedostupnom. Kako je nemoguće opisati svaku vrstu napada, u ovom dokumenti biti će opisane one najpoznatije i one koje se najčešće koriste.

4.1 Slanje prekomjernog broja SYN paketa

Slanje prekomjernog broja SYN paketa (eng. *SYN flood*) je najčešća i učinkovita vrsta DoS napada. Temelji se na iskorištavanju TCP protokola i procesa uspostavljanja TCP veze između dva računala. Kako je TCP jedan od osnovnih protokola na Internetu, ovaj napad može se primijeniti na bilo koje javno dostupno računalo.

TCP protokol omogućuje pouzdan prijenos paketa putem Interneta, a za to predviđa uspostavljanje aktivne komunikacijske veze između dva računala koja žele razmjenjivati informacije (pakete). Proces uspostavljanja veze, poznat kao trostruko rukovanje (eng. *three-way handshake*) prikazan je na sljedećoj slici.



Slika 4.1 - Uspostavljanje komunikacijske veze u TCP protokolu

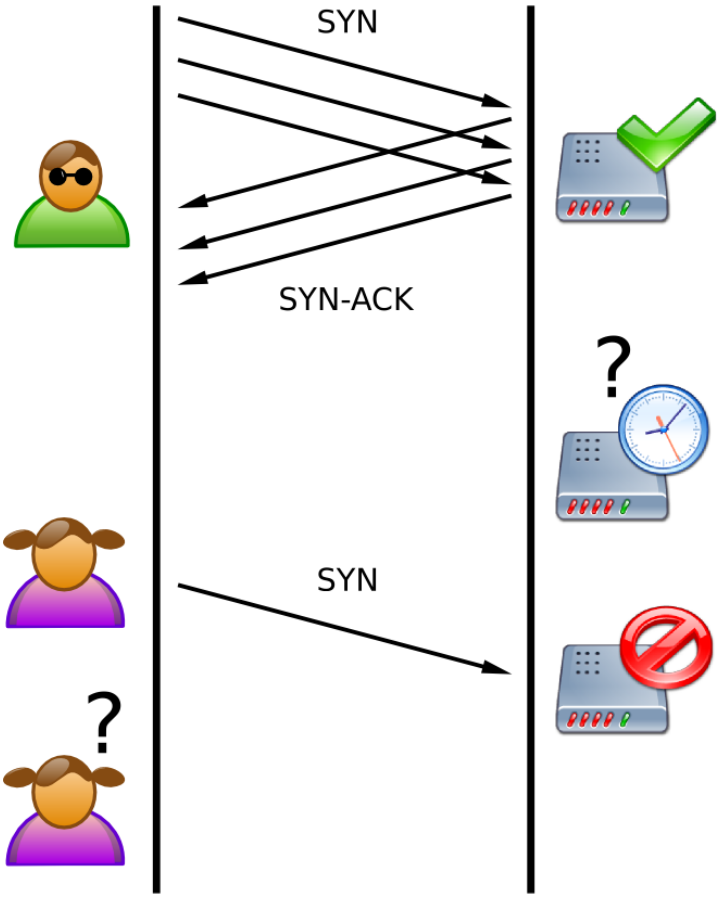
Izvor: [1]

Lijevo na slici prikazan je legitimni korisnik, koji želi uspostaviti vezu s nekim poslužiteljem na Internetu. Kako bi veza bila uspješno uspostavljena, korisnik prvo šalje poseban TCP paket koji u zaglavlju ima postavljenu SYN zastavicu. Ovaj paket poslužitelju označava da on želi uspostaviti vezu s njim. Za uspostavljanje veze poslužitelj mora odgovoriti korisniku s novim paketom koji u zaglavlju ima postavljenu SYN i ACK zastavicu (tzv. SYN-ACK paket). Kada korisnik primi SYN-ACK paket, on poslužitelju ogovara s paketom koji ima postavljenu

ACK zastavicu. Nakon toga, veza između korisnika i poslužitelja je uspostavljena i može se iskoristiti za daljnju razmjenu podataka.

Ovdje je važno napomenuti da poslužitelj i korisnik moraju održavati stanje veze. TCP protokol zahtjeva da poslužitelj zabilježi informacije o svakom pristiglom SYN paketu i nakon što pošalje SYN-ACK paket. Za takvo održavanje stanja veze potrebno je koristiti određene resurse (radna memorija, vrijeme procesora).

SYN flood temelji se na slanju velikog broja SYN paketa bez slanja posljednjeg ACK paketa poslužitelju. Provođenje napada prikazano je na sljedećoj slici.



Slika 4.2 - Slikoviti prikaz napada slanjem prekomjernog broja SYN paketa

Izvor: [1]

Na ovoj slici napadač je prikazan zelenom bojom. Njegov je cilj provesti DoS napad na poslužitelja i učinit ga nedostupnim za legitimne korisnike (ljubičasta boja). Kako bi u tome uspio, napadač šalje veliki broj SYN paketa poslužitelju. Poslužitelj svaki od tih SYN paketa vidi kao zahtjev za uspostavljanjem nove veze i na svaki odgovara s SYN-ACK paketom. Poslužitelj će potom određeno vrijeme čekati odgovor na svaki SYN-ACK paket. No, napadač neće poslati odgovor, nego će nastaviti slati SYN pakete.

Kako za obradu svakog SYN paketa poslužitelj mora odvojiti nešto resursa (vrijeme na procesoru, radna memorija…) veliki broj SYN paketa može potrošiti sve resurse na poslužitelju. Budući da poslužitelj čeka odgovor na svaki odaslani SYN-ACK paket ti resursi će neko vrijeme ostati zauzeti. U takvoj situaciji poslužitelj više ne može primiti nove SYN zahtjeve, pa ni od legitimnih korisnika, stoga on neće dobiti odgovor na svoj zahtjev za uspostavljanjem veze. Legitimnom korisniku se čini kako je poslužitelj nedostupan. Time je

napadač uspješno proveo DoS napad. Skroz dok on nastavi s slanjem velikog broja SYN paketa, vrlo je mala vjerojatnost da će poslužitelj uspjeti prihvatiti zahtjev bilo kojeg legitimnog korisnika.

Iz ovog opisa vidljivo je kako je jednostavno provesti ovakvu vrstu DoS napada. Dovoljno je osnovno poznavanje TCP protokola, a uz brojne alate situacija za napadače znatno je olakšana. Jedan od alata koji omogućava provođenje ovakvog napada je hping3. Ovaj alat, prvenstveno namijenjen mrežnim administratorima u svega nekoliko opcija omogućuje provođenje DoS napada. Npr. sljedeći oblik pozivanja alata hping3 će pokrenuti DoS napad na žrtvu s IP adresom X.

```
hping3 --flood -S X
```

Važno je napomenuti da je do sada opisana jednostavnija verzija napada zbog isticanja osnovnog mehanizma. U praksi će napadač rijetko kada primijeniti isti ovakav postupak. Naime, za napadača postoje dva osnovna problema s ovakvim pristupom:

1. Mogućnost otkrivanja identiteta – napadač sve pakete šalje s vlastitog računala i njegova IP adresa može biti zabilježena na strani poslužitelja.
2. Raspoloživost resursa – Ukoliko računalo napadača nema više raspoloživih resursa od poslužitelja napad neće uspjeti. U tom slučaju poslužitelj može obraditi više SYN paketa u jedinici vremena nego što ih napadač može poslati.

Kako bi zaštito svoj identitet napadač lažira izvorišne IP adrese svih SYN paketa koje šalje. Obično se radi o slučajno generiranim IP adresama. U tome slučaju, žrtva nikada neće dobiti pravu IP adresu napadača, ali će još uvijek morati odgovoriti na sve pristigle SYN zahtjeve budući da ne može razlikovati slučajno generirane IP adrese od legitimnih IP adresa. Većina alata za provođenje DoS napada ima opciju koja omogućuje slučajno generiranje izvorišnih IP adresa.

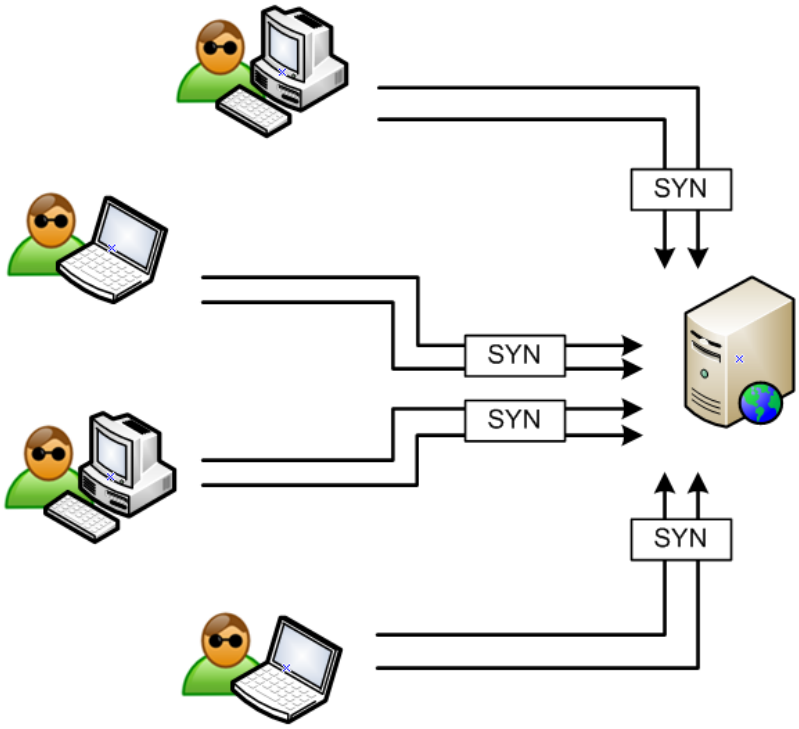
Za napadača veći problem predstavlja raspoloživost resursa. Poslužitelji su računala s više resursa i bržim mrežnim vezama od običnih kućnih računala. Kao takvima, DoS napad s pojedinog kućnog računala im ne predstavlja opasnost. Kako bi doskočio ovom problemu napadač može isti DoS napada pokrenuti na više računala u isto vrijeme.

Ovdje dolazimo do nove vrste napada – Raspodijeljeni napadi uskraćivanjem usluge (eng. *distributed denial-of-service attack - DDoS attack*). DDoS napadi su napadi uskraćivanjem usluge koji se provode protiv jedne žrtve s više različitih računala u isto vrijeme. Ukoliko napadač može pokrenuti napad s dovoljno mnogo računala čak i veliki poslužitelji se neće moći obraniti.

Kako bi prikupio dovoljan broj računala napadač razvija neki oblik zlonamjernog programa koji će se proširiti putem Interneta i pokušati zaraziti što više računala. Osim širenja, zlonamjerni program ima mogućnost provođenja barem jedne vrste DoS napada. On napadaču omogućuje kontrolu nad zaraženim računalom što uključuje i pokretanje DoS napada s tog računala.

Takav zlonamjerni program može zaraziti veliki broj računala i napadaču omogućiti da ih poveže u velike mreže koje se nazivaju *botnet* mrežama. Zabilježene su *botnet* mreže koje imaju nekoliko desetaka pa i stotina tisuća računala.

Napadač može *botnet* mrežu iskoristiti za pokretanje DDoS napada. Slijedi slikoviti prikaz jednog DDoS napada na web poslužitelj.



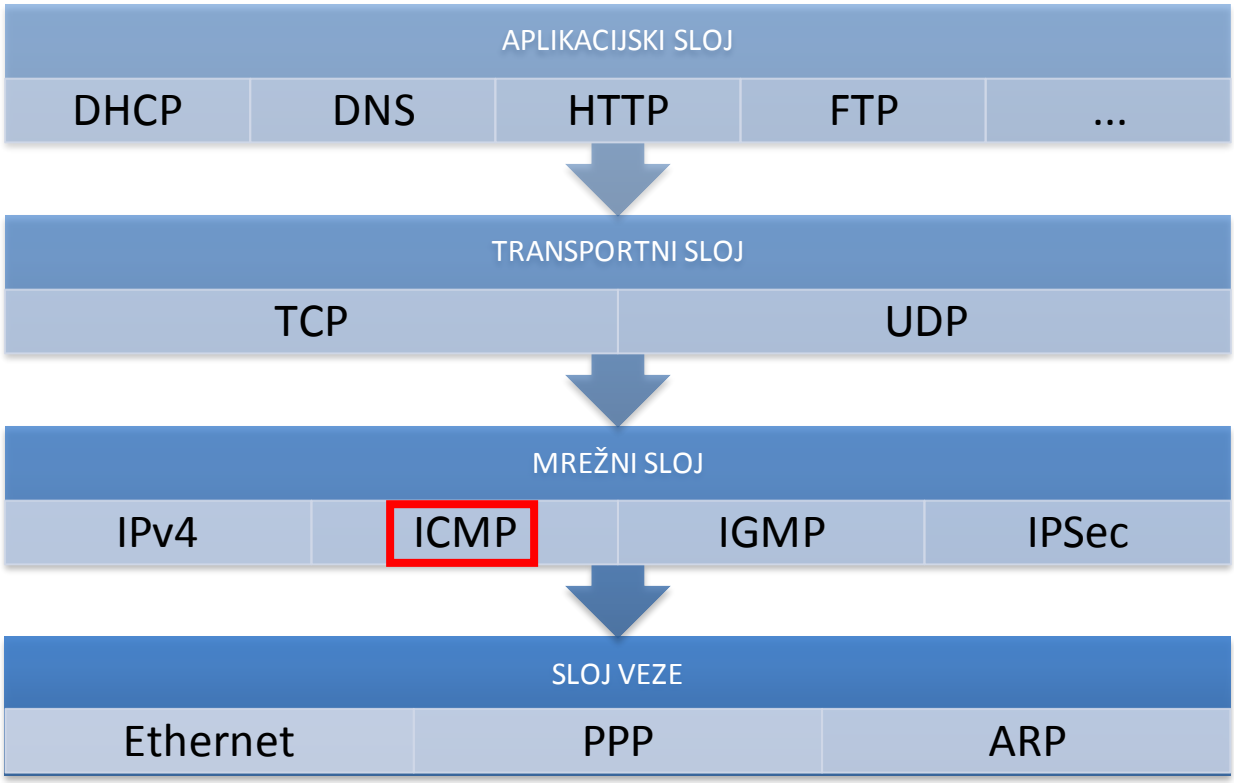
Slika 4.3 - Raspodjeljeni napad uskraćivanjem usluge

Velike *botnet* mreže koje koriste SYN flood tehniku DoS napada i pri tome generiranju slučajne izvorišne IP adrese za svaki SYN paket danas su čest i opasan oblik provođenja DoS napada. To se pogotovo odnosi na *botnet* mreže s složenom strukturom upravljanja i velikim brojem zaraženih računala.

Dodatni problem za sigurnosne stručnjake koji pokušavaju spriječiti razvoj takvih aktivnosti je nemogućnost otkrivanja identiteta napadača. Ukoliko *botnet* mreža ima dobro razrađenu strukturu upravljanja gotovo je nemoguće otkriti tko stoji iza nje. Osim tehničkih, postoje i pravni problemi prilikom razotkrivanja identiteta napadača. U većini država napad uskraćivanjem usluge tretira se kao kazneno djelo stoga žrtva može tražiti zaštitu zakonodavca. No problem nastaje u činjenici da se računala s kojih se providi napad nalaze u raznim državama, a sam napadač također može biti u drugoj državi. Njegovo razotkrivanje zahtjeva suradnju na većoj razini od pojedine države, a to je gotovo nemoguće ostvariti u razumnom vremenu.

4.2 Slanje velikog broja ICMP echo zahtjeva

Slanje velikog broja ICMP echo zahtjeva još je jedna od raznih vrsta DoS napada. Ova vrsta napada zasniva se na korištenju ICMP protokola za slanje velikog broja paketa na mrežnu adresu žrtve. ICMP je protokol koji se koristi za slanje različitih kontrolnih poruka između čvorova na računalnoj mreži. Za razliku od TCP protokola on se nalazi na mrežnom sloju standardnog TCP/IP modela. Sljedeća slika prikazuje njegov odnos s nekim drugim protokolima unutar TCP/IP mrežnog modela. ICMP protokol označen je crvenom bojom.



4.4 - Prikaz slojeva unutar TCP/IP modela

ICMP protokol ne uspostavlja vezu između dva računala, niti se koristi za razmjenu informacija. Zbog toga, obrada ICMP paketa zahtjeva znatno manje resursa i gotovo je trenutačna. Nema uspostavljanja veze i očuvanja stanja kao što je to bio slučaj kod trostrukog rukovanja u TCP protokolu. Svaki napad uskraćivanjem usluge putem ICMP protokola nije usmjeren na iskorištavanje resursa žrtve nego na zagušenje mrežne veze s velikim brojem paketa.

Obično se u tim napadima šalju ICMP paketi tipa *echo request*. To su paketi koji u ICMP zaglavlju imaju kodnu oznaku broj 8. Oni od primatelja zahtijevaju da odgovori s ICMP *echo reply* paketom. Napadač koji šalje veliki broj ICMP *echo request* paketa može uspješno provesti napad uskraćivanjem usluge samo ukoliko ima pristup bržoj mrežnoj vezi nego žrtva. U tome slučaju on će komunikacijski kanal do žrtve prepuniti s ICMP *echo request* paketima, pa više niti jedan zahtjev legitimnog korisnika neće moći doći do žrtve.

Postoje brojni alati koji automatiziraju slanje velikog broja ICMP paketa s pojedinog računala. Neki alati omogućuju slanje samo ICMP *echo request* paketa, dok drugi omogućuju slanje proizvoljnog ICMP paketa. Jedan takav alat je i hping3 za Linux operacijski sustav kojemu se s opcijom *--flood* može zadati slanje velikog broja ICMP paketa.

4.3 Napad slanjem velikog broja UDP paketa

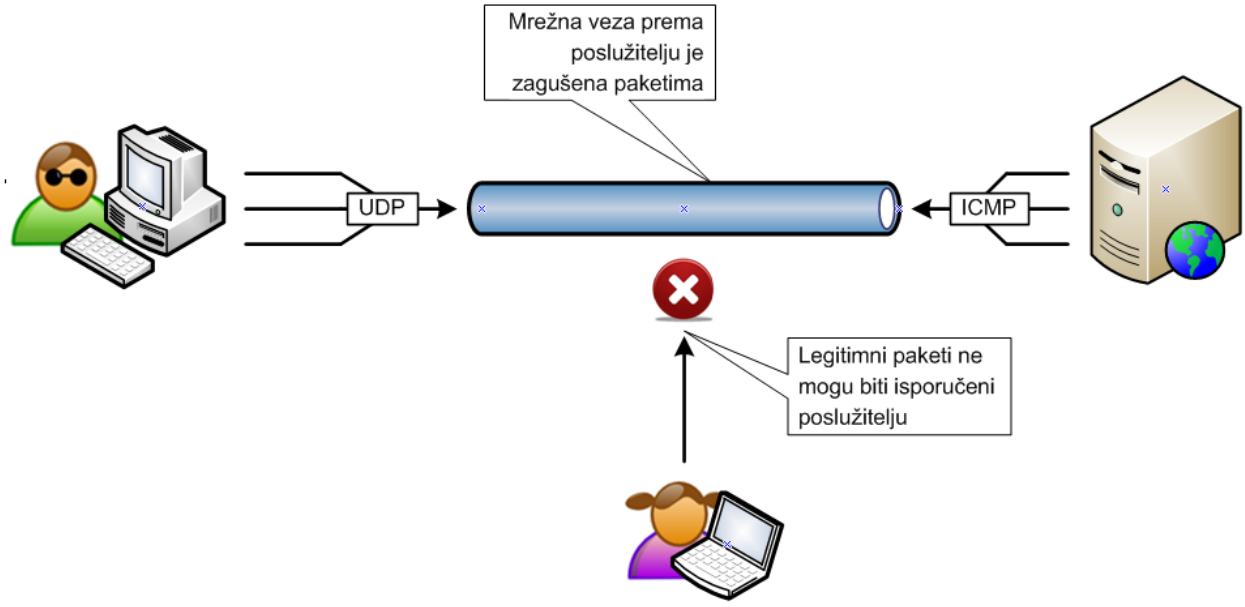
UDP protokol, kao i TCP, nalazi se na transportnom sloju standardnog TCP/IP modela. On omogućuje razmjenu paketa između dva računala na mreži bez prethodnog uspostavljanja komunikacijskog kanala i stvaranja sesije. Zbog toga UDP ne omogućuje pouzdan prijenos paketa budući da oni na odredište mogu doći u krivom redoslijedu, biti duplicirani ili jednostavno nestati bez bilo kakve obavijesti.

DoS napad slanjem velikog broja UDP paketa učinkovitiji je nego napad slanjem TCP SYN paketa. Razlog tomu je problem u otkrivanju i prevenciji napada. Veliki broj uređaja dizajniranih za zaštitu od DoS napada ima problema u razlikovanju legitimnog od zlonamjernog UDP prometa baš zbog toga što UDP protokol ne zahtjeva održavanje stanja.

Sam napad temelji se na slanju velikog broja UDP paketa odabranoj žrtvi. Svaki UDP paket ima slučajno generiran odredišni port. Da bi žrtva obradila takav UDP paket ona mora:

- Provjeriti koja aplikacija koristi navedeni UDP port
- Zaključiti da niti jedna aplikacija ne koristi navedeni UDP port
- Odgovoriti s ICMP *destination unreachable* paketom

Pretpostavka napada je da će za veliki broj UDP paketa žrtva odgovarati s velikim brojem ICMP paketa i time zagušiti vlastitu komunikacijsku vezu prema internetu. Napad je shematski prikazan na sljedećoj slici.



4.5 - Prikaz napada slanjem UDP velikog broja UDP paketa

Kao i kod svih napad koji su do sada spomenuti napadač može generirati slučajnu izvorišnu IP adresu u paketima i time zaštititi svoju privatnost. Također i ovaj napad se može izvesti na distribuiran način čime se povećavaju šanse napadaču da onemogući rad pojedine žrtve.

Kao što je bio slučaj s SYN i ICMP *flood* napadima alat hping3 može pokretati i napad slanjem velikog broja UDP paketa. Za to je prilikom pokretanja alata dovoljno postaviti opciju *--udp*.

4.4 Ostali napadi

Napadi koji su do sada opisani najčešći su i najpoznatiji DoS napadi. Njihovo izvođenje s tehničke strane relativno je jednostavno i vrlo su učinkoviti protiv nepripremljenih žrtava. No, postoje i drugi načini provođenja mrežnih DoS napada. Ovdje je, kao svojevrstan pregled, navedeno nekoliko njih.

Napad slanjem velikog broja TCP ACK paketa

Kao i kod napada slanjem velikog broja TCP SYN paketa žrtva je preplavljena velikim brojem TCP paketa. No kod ovog napada ne radi se o SYN paketima već o paketima koji imaju postavljenu ACK zastavicu u TCP zaglavlju. Cilj je jednak – zauzeti sve resurse žrtve i onemogućiti obradu legitimnih zahtjeva. Ovisno o tome koji operacijski sustav žrtva koristi, moguće je da će ona na svaki TCP ACK paket koji je poslan na zatvoreni TCP port odgovoriti s TCP RST paketom, u tom slučaju generira se dodatni promet koji pospješuje sam napad.

Napad slanjem velikog broja NULL paketa

NULL paket je onaj TCP paket koji nema postavljenu niti jednu zastavicu. Ovaj napad zasniva se na slanju velikog broja takvih paketa žrtvi. Cilj napada jednak je kao i kod bilo kojeg drugog DoS napada.

Napad slanjem slučajno generiranih TCP zaglavlja

Ovaj napad zasniva se na slanju velikog broja TCP paketa koji imaju slučajne vrijednosti pojedinih atributa u zaglavlju. Zabilježeno je da ovakav napad osim iskorištavanja resursa žrtve može u potpunosti srušiti operacijski sustav žrtve budući da dolazi do neispravne obrade TCP paketa. Postizanje takvog rezultata ovisi o operacijskom sustavu koji žrtva koristi.

Napad slanjem polu-ispravnih IP zaglavlja

Ovaj napad sličan je napadu u kojem se žrtvi šalje veliki broj paketa s slučajno generiranim TCP zaglavljem, samo je u ovom napadu slučajno generirano IP zaglavlje. Naravno, nisu sva polja unutar IP zaglavlja slučajno generirana budući da bi to spriječilo paket da dođe do žrtve. Cilj napadača je izraditi „neuobičajen“ IP paket koji žrtva neće moći pravilno obraditi, što će uzrokovati rušenje ili zamrzavanje operacijskog sustava.

Hibridni napadi

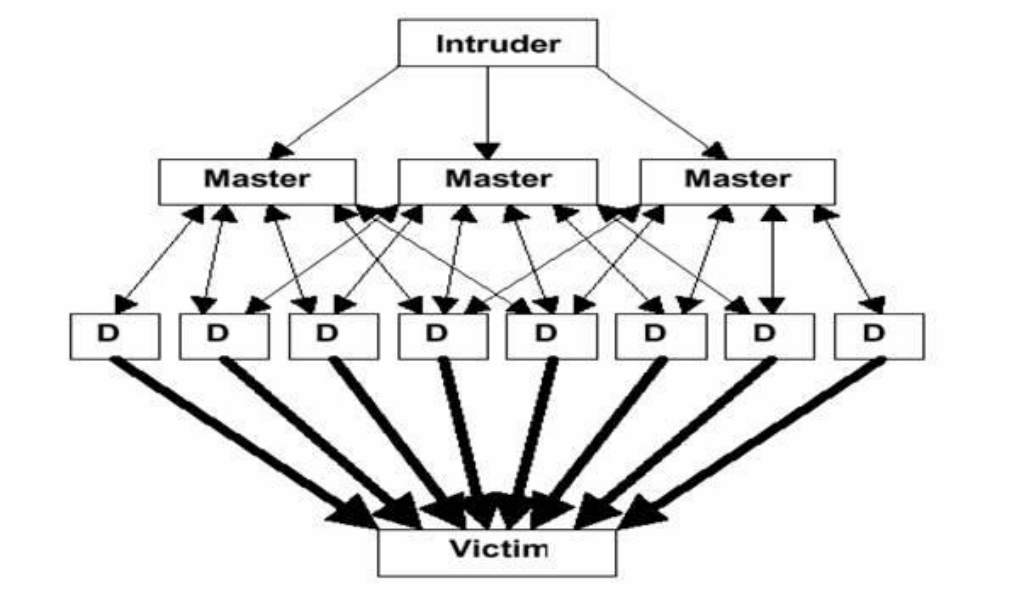
Hibridni napadi kombinacija su dva ili više DoS napada. Moguće je u istom trenutku na istu žrtvu pokrenuti nekoliko različitih DoS napada, a napadači to obično koriste da što prije onemoguće rad žrtve. Iako je moguća gotovo bilo koja kombinacija napada, najčešće se koristi napad slanjem velikog broja TCP SYN paketa, napad slanjem velikog broja UDP paketa i napad slanjem velikog broja ICMP paketa. Uz napad slanjem velikog broja UDP paketa ovo je najopasniji oblik DoS napada.

4.5 Stacheldraht

Kada je riječ o napadima uskraćivanjem usluge dobro je spomenuti jedan poznati alat koji omogućuje provođenje svih do sada nabrojanih vrsta napada. Alat se zove *Stacheldraht* što na njemačkom znači „bodljikava žica“. Prvi puta se pojavio 1999. godine, a njegova zadnja verzija zabilježena je 2000. godine. Pisan je za Solaris i Linux operacijske sustave.

Iako je alat star više od jednog desetljeća korisno ga je spomenuti u kontekstu penetracijskog testiranja. I dok je u vrijeme svog nastanka alat možda bio korišten u ilegalne svrhe, danas to više nije slučaj. Kriminalci koji provode DoS napade većinom za to koriste velike botnet mreže koje uspostavljaju širenjem raznih vrsta zlonamjernih programa. *Stacheldraht* je koristan administratorima i sigurnosnim stručnjacima koji provode penetracijska testiranja budući da s njime mogu provjeriti otpornost računalne mreže na DoS napade.

Osim što *Stacheldraht* omogućuje provođenje svih do sada navedenih vrsta DoS napada alat ima i nekoliko dodatnih mogućnosti. Jedna od njih je slojevita arhitektura upravljanja prikazana na sljedećoj slici.



Slika 4.6 - Prikaz funkcioniranja Stacheldrahta

Izvor: [2]

Stacheldraht za pokretanje napada koristi maleni program nazvan agent. Agenti se instaliraju na ona računala s kojih se želi pokrenuti napad. Na slici su agenti označeni slovom D. Uz agente postoje i upravitelji (eng. Master) koji kontroliraju jednog ili više agenta. Na najvišoj razini je korisnik koji koristi upravitelje za kontrolu agenata. Korisnik ima posebno razvijen klijent kojim se može spojiti na pojedinog upravitelja kako bi mu izdao naredbe.

Treba istaknuti da je komunikacija između korisnika i upravitelja kriptirana i prikrivena budući da se za komunikaciju koristi ICMP protokol. Naredbe upraviteljima smještaju se unutar ID atributa ICMP zaglavlja, a svi parametri se nalaze unutar *Optional data* atributa.

5 Zaštita od DoS napada

Kako su DoS napadi postali izrazito popularni razvili su se brojni mehanizmi zaštite. No, usprkos brojnošću i kreativnosti tih mehanizama niti jedan ne pruža apsolutnu zaštitu protiv DoS napada. Pogotovo se to odnosi na DDoS napade velikih razmjera. Jako je teško i skupo dizajnirati sustav koji može ostati funkcionalan usprkos ogromnoj količini prometa koji dolazi s nekoliko stotina tisuća različitih računala. Većina mehanizama za zaštitu može samo smanjiti rizik ili štetu koja nastaje DoS napadom. Također, uvijek valja razmisliti o implementaciji određenog mehanizma zaštite. Pri tome bi glavni kriterij trebao biti isplativost. Ukoliko je zaštita skuplja nego resurs koji se štiti onda je ona nepotrebna.

5.1 SYN kolačići

SYN kolačići razvijeni su kao zaštita od DoS napada slanjem velikog broja SYN paketa. Cilj ove zaštite je da oslobodi resurse koje poslužitelj mora alocirati za obradu pojedinog SYN paketa. SYN kolačići omogućuju poslužitelju da prihvati svaki SYN zahtjev koji mu dođe, na njega odgovori s SYN/ACK paketom i potom zanemari resurse alocirane za taj SYN zahtjev. Tek ukoliko poslužitelj dobije nazad ACK od klijenta on alocira resurse i u potpunosti uspostavlja vezu.

Kako poslužitelj može zanemariti resurse na nakon slanja SYN/ACK paketa, a da još uvijek zna uspostaviti vezu ukoliko klijent pošalje ACK zahtjev? Odgovor leži u načinu na koji poslužitelj šalje SYN/ACK paket. Prilikom slanja tog paketa poslužitelj će u slijedni broj kodirati informaciju potrebnu za rekonstrukciju pristiglog SYN paketa. Jednom kada klijent pošalje ACK paket poslužitelj će iz kodirane informacija moći rekonstruirati originalni SYN paket i u potpunosti uspostaviti vezu.

Na ovaj način će poslužitelj u potpunosti zanemariti svaki SYN paket koji pošalje napadač budući da on nikada ne odgovara s ACK paketom. Svi legitimni korisnici će bez obzira na napad moći uspostaviti vezu s poslužiteljem.

Jezgra Linux operacijskog sustava uključuje podršku za SYN kolačiće, a oni se jednostavno mogu uključiti sljedećom naredbom:

```
echo 1 > /proc/sys/net/ipv4/tcp_syncookies
```

Uporaba SYN kolačića može omogućiti dostupnost sustava čak ukoliko se on nalazi pod DoS napadom. No, ova metoda zaštite ima svoje granice. Iako uporaba SYN kolačića ubrzava obradu TCP paketa, poslužitelj još uvijek troši određene resurse da bi prihvatio paket i poslao odgovor. Osim toga, mrežna veza koju poslužitelj koristi ima ograničen kapacitet. Zbog toga će dovoljno veliki DoS napad onemogućiti rad i onih poslužitelja koji koriste SYN kolačiće.

5.2 TCPCT

TCPCT je kratica za TCP Cookie Transaction. Riječ je o proširenju TCP protokola čiji je cilj pružanje zaštite od DoS napada slanjem prekomjernog broja TCP SYN paketa. S tehničke strane proširenje funkcionira slično kao i mehanizam SYN kolačića. No, za razliku od SYN kolačića, ovo proširenje zahtjeva implementaciju podrške na obje strane koje sudjeluju u komunikaciji.

Mehanizam zaštite temelji se na razmjeni kolačića između obje strane koje sudjeluju u komunikaciji. Pri tome ona strana koja prima komunikaciju ne održava stanje, već je za to zadužena strana koja započinje komunikaciju. Korištenjem TCPCT-a TCP zaglavlje dobiva dodatno polje u koje se spremaju kolačići jedne i druge strane. U tim kolačićima zapisane su informacije o stanju veze, te se na taj način stanje veze može rekonstruirati prilikom primanja paketa.

Ona strana koja prima inicijalni SYN paket u njemu će dobiti i kolačić koji opisuje opcije i stanje veze. Na taj SYN paket potrebno je poslati SYN/ACK paket koji će uz inicijalni kolačić sadržavati i kolačić s opcijama strane koja je primila SYN paket. Poslužitelj potom može zanemariti sve resurse potrebne za održavanje stanja veze. Ukoliko dobije ACK paket koji sadrži odgovarajuće kolačiće stanje veze može se rekonstruirati iz njih i komunikacija nastaviti normalnim tokom.

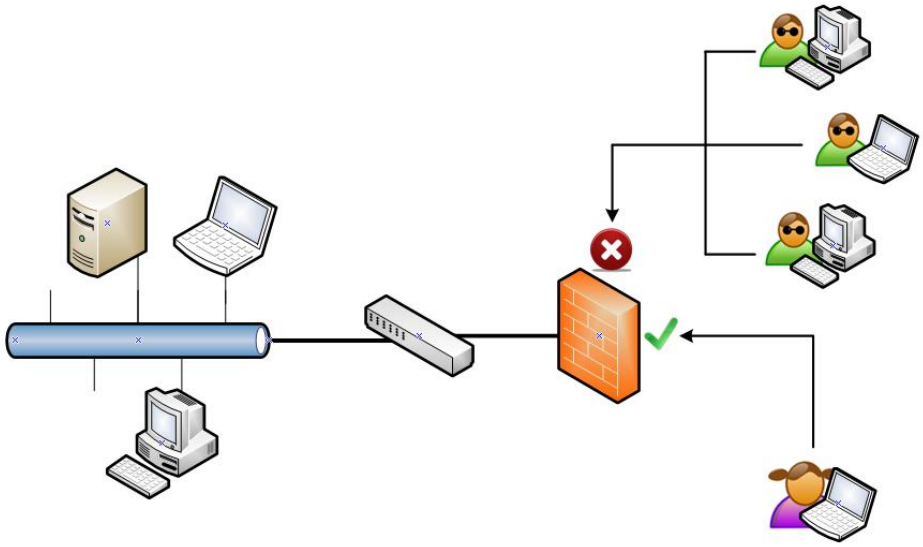
Jednako kao i SYN kolačići ovaj mehanizam smanjuje rizik od provođenja uspješnih DoS napada slanjem velikog broja SYN paketa. Razlog tomu je činjenica da za održavanje stanja veze nije potrebno koristiti resurse poslužitelja.

Nažalost i ovaj mehanizam ne rješavanja problem DoS napada, već samo od napadača zahtjeva da pokrene napad većih razmjera nego onaj napad koji bi uskratio uslugu da se TCPCT ne koristi.

5.3 Uporaba mogućnosti mrežnih uređaja

Različiti mrežni uređaju kao što su vatrozid, preklopnik, usmjerivač ili IPS imaju različite mogućnosti ograničavanja ili smanjivanja utjecaja DoS napada. Prilikom implementacije mreže svakako je potrebno iskoristiti te mogućnosti.

Vatrozid može ograničiti mrežni promet temeljem niza pravila i karakteristika, slično vrijedi i za preklopnike ili IPS uređaje. Moguće je definirati maksimalnu protočnost podatkovne veze. Ograničiti broj istodobnih veza prema nekom poslužitelju. Mogućnosti mrežnih uređaja ima mnogo, a kombinacijom s mogućnostima zaštite na samoj žrtvi rizik i štetni utjecaj DoS napada može se znatno smanjiti. Mrežni uređaji koji imaju ove mogućnosti postavljaju se između poslužitelja koji se želi zaštiti i izlaza na javni Internet. Oni će potom blokirati DoS napad tako da on nikada neće doći do poslužitelja. Takva situacija prikazana je na sljedećoj slici.



5.1 - Prikaz vatrozida u sprečavanju napada uskraćivanjem usluge

Različiti uređaji imaju različite mogućnosti, npr. IPS uređaj radi na aplikacijskom sloju i može biti učinkovit protiv DoS napada na pojedine aplikacije (vidi poglavlje 6). Uređaji također dolaze u različitim izvedbama. Tako je svaki uređaj moguće instalirati kao zaseban komad opreme, ali je isto tako moguće imati uređaj koji je ujedno vatrozid i IPS sustav.

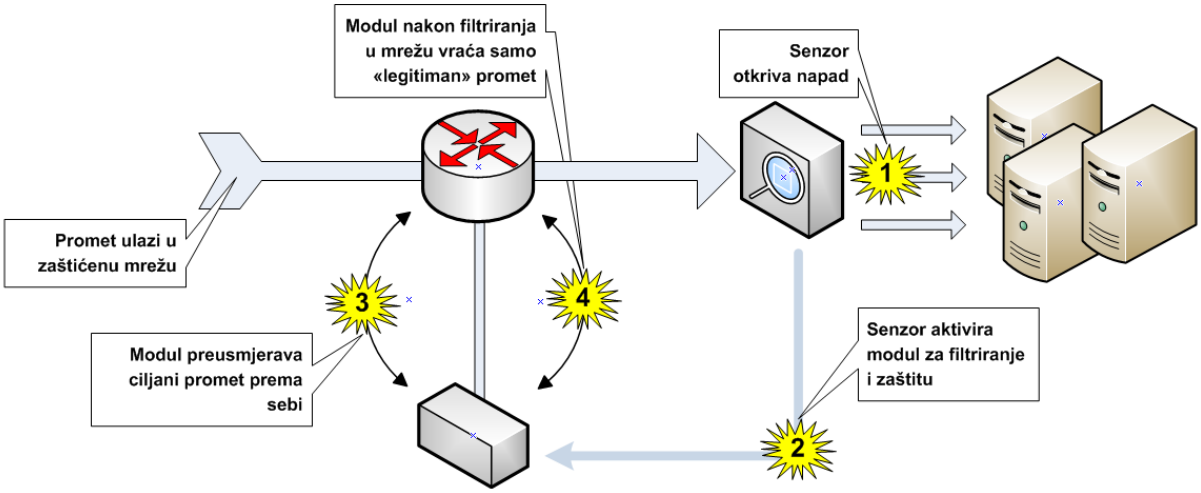
Važno je istaknuti da ovi uređaji ne mogu pružiti apsolutno rješenje problema s DoS napadima. Oni su ograničeni činjenicom da nisu dizajnirani isključivo za borbu s DoS napadima. Za učinkovitu zaštitu potrebno je posegnuti za naprednijim uređajima.

5.4 Napredni uređaji

Ovisno o potrebama i zahtjevima za dostupnošću moguće je implementirati puno bolju zaštitu od DoS napada nego što to pružaju uobičajeni mrežni uređaji ili softverske postavke na samom poslužitelju. Ovdje je riječ o specijaliziranim mrežnim uređajima koji su izrađeni isključivo za borbu protiv DoS napada. Sustavi za zaštitu temeljeni na takvim uređajima sastoje se obično iz dva djela:

- Modul za filtriranje i zaštitu – Uređaj koji preusmjerava dolazni promet prema meži i provodi filtriranje
- Senzor – Uređaj koji prati promet na ključnim točkama u mreži i obavještava modul za filtriranje i zaštitu o pojavi napada.

Sljedeća slika zorno prikazuje ovakav sustav u radu.



Slika 5.2 - Prikaz naprednog rješenja za borbu protiv DDoS napada

Razlikovanje legitimnog od zlonamjernog prometa temelji se na učenju prometa. Modul za filtriranje i zaštitu nema statička pravila prema kojima filtrira promet već koristi predloške koji oslikavaju normalan promet na mreži i redovito se ažuriraju.

Uz činjenicu da se takvi uređaji temelje na učenju prometa, valja istaknuti kako oni imaju izrazito veliku procesnu moć i mogu obrađivati pakete na brzim mrežnim vezama, stoga su oni iznimno učinkoviti u zaustavljanju DDoS napada.

U obrani od različitih DoS napada mogu pomoći i uređaji za raspodjelu opterećenja (eng. *load-balancing*). Raspodjela opterećenja je tehnika koja se koristi za pružanje jedinstvene Internet usluge s više različitih poslužitelja. Krajnji korisnik usluge ne može razlikovati s kojeg poslužitelja mu se usluga isporučuje budući da je za njega raspodjela opterećenja u potpunosti transparentna.

Uređaj za raspodjelu opterećenja brine se o tome da svi dolazni zahtjevi za pojedinom uslugom budu ravnomjerno raspoređeni na sve dostupne poslužitelje. Time se smanjuje opterećenost pojedinog poslužitelja. Zbog ovakvog načina funkcioniranja uređaji za raspodjelu opterećenja mogu smanjiti rizik od DoS napada. Mnogi takvi uređaji imaju ugrađene mogućnosti za prevenciju DoS napada. Kao jedan primjer možemo istaknuti prevenciju napada slanjem prekomjernog broja TCP SYN paketa. Uređaj za raspodjelu

opterećenja kod takvog napada neće proslijediti vezu pozadinskom poslužitelju skroz dok se proces trostrukog rukovanja ne završi. Osim toga, sama činjenica da se takvi uređaji brinu da veliki broj zahtjeva ne isporučuje samo jedan poslužitelj može smanjiti rizik od DoS napada.

5.5 Dizajn računalne mreže

Već prilikom dizajna računalne mreže potrebno je misliti na zaštitu od DoS napada. Mrežu je potrebno dizajnirati tako da se osigura dodatni komunikacijski kanal s kojega se može pristupiti administraciji poslužitelja i mrežnih uređaja. Taj dodatni komunikacijski kanal mora biti dostupan i za vrijeme trajanja DoS napada. Njega je stoga potrebno izgraditi na različitoj mrežnoj infrastrukturi od one koju koriste legitimni korisnici za pristup poslužiteljima.

Ukoliko DoS napadi mogu prouzročiti veliku štetu pojedina organizacija treba razmisliti o uvođenju rezervnog IP adresnog prostora. Taj rezervni blok može sadržavati kopiju svih poslužitelja, a može postati aktivan u trenutku kada počne DoS napad na primarni blok. Naravno, poslužitelji koji se nalaze na tom rezervnom bloku moraju koristiti zasebnu infrastrukturu za pristup javno dostupnom internetu.

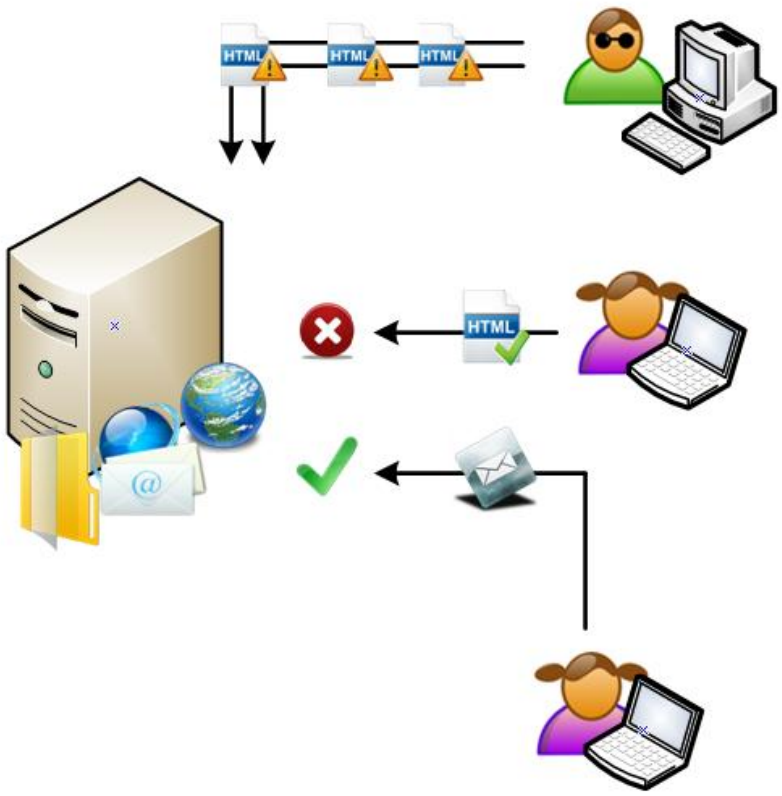
6 DoS napadi na razini aplikacije

Svaki, do sada, opisani oblik DoS napada temeljio se na slanju velikog broja paketa putem nekog protokola na mrežnom ili transportnom sloju. Kao rezultat toga, žrtva bi postala nedostupna za svoje legitimne korisnike bilo zbog potrošnje vlastitih resursa ili zbog zagušenja mrežne veze koju ona koristi. Također, koliko god servisa žrtva ima, svi oni bili bi nedostupni. Legitimnom korisniku činilo bi se kako žrtva uopće ne postoji na Internetu.

Postoje i DoS napadi koji su usmjereni protiv određene aplikacije na poslužiteljima. Oni koriste pojedine aplikacijske protokole i omogućuju uskraćivanje samo onih usluga koje aplikacija nudi korisnicima. Npr. DoS napad na web poslužitelj će onemogućiti prikaz web stranica svim klijentima, dok će u istom trenutku poslužitelj za elektroničku poštu funkcionirati bez poteškoća.

Uspješnost takvih napada ovisi o kvaliteti ili konfiguraciji pojedine aplikacije. Može se dogoditi da je ista aplikacija na jednom poslužitelju ranjiva, dok na drugom nije budući da su različito podešene.

Kao primjer DoS napada na aplikacijskoj razini moguće je istaknuti napad na web poslužitelje putem HTTP protokola. Jedan oblik takvog napada temelji se na otvaranju velikog broja HTTP veza prema web poslužitelju i držanju tih veza otvorenim. Veze se drže otvorenima slanjem dijelova valjanog HTTP zahtjeva. Jednom kada se otvori dovoljan broj veza, web poslužitelj će prestati prihvaćati zahtjeve za novim vezama. Ukoliko napadač stalno otvara nove veze i drži ih otvorenim, niti jedan legitimni korisnik neće moći pristupiti web poslužitelju. Na slici je prikazana anatomija ovog napada.



6.1 - Prikaz napada uskraćivanjem usluge na pojedinu aplikaciju

Napadač pokreće napad uskraćivanjem usluge i pri tome šalje određeni broj nepotpunih HTTP zahtjeva web poslužitelju. Na slici su nepotpuni zahtjevi prikazani s znakom upozorenja, budući da se oni rijetko pojavljuju prilikom normalnog rada web poslužitelja. Za svaki nepotpun HTTP zahtjev web poslužitelj će pričekati određeno vrijeme dok klijent ne pošalje ostatak zahtjeva. Pri tome će nastaviti zaprimati nove zahtjeve. Jednom kada napadač pošalje dovoljan broj zahtjeva svi resursi web poslužitelja biti će zauzeti i on više neće moći primati nove zahtjeve.

U tom trenutku svaki legitimni korisnik koji pokuša pristupiti nekoj web stranici na tom web poslužitelju će biti odbijen. Skroz dok napadač ne prekine napad, web poslužitelj će ostati nedostupan.

Na slici je prikazan i legitimni korisnik koji koristi poslužitelj elektroničke pošte. Iako je web poslužitelj pod DoS napadom, poslužitelj elektroničke pošte može funkcionirati normalno i redovito obrađivati zahtjeve svojih klijenata. Razlog tomu leži u intenzitetu napada na web poslužitelj. Svi DoS napadi koji rade na aplikacijskoj razini ne generiraju iznimno mnogo mrežnog prometa i time ne zagušuju resurse cijelog računala već samo određene aplikacije.

Npr. kako bi ovakav napad bio u potpunosti uspješan za standardnu konfiguraciju Apache web poslužitelja dovoljno je poslati nekoliko stotina djelomičnih HTTP zahtjeva svakih 5 minuta. Takva količina prometa ne predstavlja veliki problem ni slabijim računalima.

6.1 Zaštita od aplikacijskih DoS napada

Za razliku od DoS napada na razini mreže, DoS napadi na razini aplikacije ne predstavljaju veliki rizik budući da za njih postoje potpuno učinkovite metode zaštite. U najvećem broju slučajeva za zaštitu je dovoljno podesiti konfiguraciju same aplikacije. Tako je potrebno ograničiti maksimalan broj istodobnih veza koje će aplikacija podržavati ili podesiti maksimalno trajanje pojedine veze.

Za primjer je moguće istaknuti konfiguraciju Apache web poslužitelja. S standardnom instalacijom Apache web poslužitelj će prije gašenja veze čekati 300 sekundi. Ovakva velika vrijednost je nepotrebna i promjenom konfiguracijske opcije TimeOut unutar konfiguracijske datoteke *httpd.conf* može se smanjiti. Time će se znatno smanjiti rizik od provođenja DoS napada na sam Apache poslužitelj.

Ukoliko aplikacija ne nudi konfiguracijske opcije kojima bi se mogao smanjiti rizik od provođenja DoS napada, moguće je za to iskoristiti neki vanjski uređaj kao što je vatrozid ili IPS. Vatrozid može ograničiti maksimalan broj istodobnih veza prema web poslužitelju ili maksimalno trajanje uspostavljene veze, a IPS može prepoznati različite napade na aplikaciju na aplikacijskom sloju mrežnog modela.

7 Zaključak

Konačni zaključak o napadima s uskraćivanjem usluga najlakše je izreći kroz nekoliko točaka koje je važno zapamtiti:

- Napadi uskraćivanjem usluga ne zahtijevaju veliko tehničko znanje za provođenje i napadaču ne omogućuju dobivanje kontrole nad žrtvom.
- Iako postoji mnoštvo različitih vrsta DoS napada, samo nekoliko ih je popularnih. Među njima, najpoznatiji i najkorišteniji je napad slanjem velikog broja TCP SYN paketa. Posebno je opasan ukoliko se odvija kao distribuirani napad uskraćivanjem usluge. U takvom obliku napada pronalaženje s tehničke strane teško je ostvarivo.
- Za učinkovitu zaštitu potrebno je razviti niz mjera i pravilno ih implementirati. Pri tome je važno zapamtiti da ne postoji savršeno rješenje budući da dovoljno veliki napad može zaustaviti rad i najbržih poslužitelja.
- Postoje i DoS napadi koji funkcioniraju na aplikacijskom sloju. Oni predstavljaju znatno manji rizik od standardnih DoS napada i zaštitu je moguće postići pravilnom konfiguracijom pojedinih aplikacija.

8 Literatura

[1]. **Wikipedia.** SYN Flood. *Wikipedia.* [Mrežno] Wikipedia. [Citirano: 10. 9 2010.] http://en.wikipedia.org/wiki/Syn_flood.

[2]. **Cisco Systems.** *Cisco DDoS mitigation service provider solutions.* s.l. : Cisco Systems, 2005.

[3]. **Cheng, Geoffrey.** Malware FAQ: Analysis on DDOS tool Stacheldraht v1.666. *Malware FAQ: Analysis on DDOS tool Stacheldraht v1.666.* [Mrežno] Sans. [Citirano: 21. 9 2010.] http://www.sans.org/security-resources/malwarefaq/stacheldraht.php.

[4]. **CERT.** Denial of Service Attacks. *Denial of Service Attacks.* [Mrežno] CERT. [Citirano: 20. 9 2010.] http://www.cert.org/tech_tips/denial_of_service.html.

[5]. **Wikipedia.** Load balancing. *Load balancing.* [Mrežno] [Citirano: 22. 9 2010.] http://en.wikipedia.org/wiki/Load_balancing_%28computing%29.

[6]. **Cisco Systems.** How does Load Balancing Work? *How does Load Balancing Work?* [Mrežno] [Citirano: 23. 9 2010.] http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080094820.shtml.