HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Napadi uskraćivanjem resursa

CCERT-PUBDOC-2006-07-162

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Ovaj dokument predstavlja vlasništvo CARNet-a (CARNet CERT-a). Namijenjen je za javnu objavu, njime se može svatko koristiti, na njega se pozivati, ali samo u originalnom obliku, bez ikakvih izmjena, uz obavezno navođenje izvora podataka. Korištenje ovog dokumenta protivno gornjim navodima, povreda je autorskih prava CARNet-a, sukladno Zakonu o autorskim pravima. Počinitelj takve aktivnosti podliježe kaznenoj odgovornosti koja je regulirana Kaznenim zakonom RH.

Sadržaj

1. Uvod

Napadi uskraćivanja resursa (eng. DoS - *Denial of Service*) su aktivnosti poduzete od strane zlonamjernih korisnika sa ciljem onemogućavanja ispravnog funkcioniranja različitih računalnih i/ili mrežnih resursa čime određene usluge postaju nedostupne. Često korišten izraz u hrvatskoj literaturi je i DoS stanje, a odnosi se na vremenske trenutke nepravilnog rada ili potpune onemogućenosti funkcioniranja aplikacija i računalnih ili mrežnih usluga. Činjenica da je Internet izgrađen od konačnog broja mrežnih komponenata te da računalni sustavi ne raspolažu s neograničenim količinama procesne moći, pridonosi ishodima ovakvih napada.

Dokument je koncipiran tako da opiše većinu poznatih DoS napada i pri opisu pruži kraći osvrt na načine obrane od istih. Pri tome su napadi grupirani prema logičnoj podjeli, što nije uvijek moguće jasno izvesti budući da se nekim napadima svojstva mogu ubrojiti u jednu ili drugu skupinu. Na kraju dokumenta opisane su i osnovne prevencijske i tehničke metode zaštite od DoS napada.

2. DoS napadi

Vrijeme kada se korisnicima Interneta moglo vjerovati je prošlo. Nažalost, uz tako velik broj korisnika svakodnevno priključenih na Internet, među njima se razotkriva sve veći broj zlonamjerno orijentiranih korisnika. Ti pojedinci kojima je u interesu onemogućavati normalno korištenje računala i Interneta, čine to različitim oblicima devijantnog ponašanja. Jedan od takvih devijantnih oblika njihovog ponašanja su i napadi zasnovani na uskraćivanju resursa (DoS). Razlozi za pokretanje ovakvih napada mogu biti raznoliki, a ne zahtijevaju veliko stručno predznanje jer ih je moguće izvršavati koristeći različite alate pisane upravo za ovakve svrhe, ali isto tako i alate čija je temeljna namjena sasvim drugačija. Čest razlog za njihovo pokretanje je uglavnom obijest zlonamjernih korisnika.

Najčešći oblici napada usmjereni su u pravilu na pojedine web stranice u svrhu onemogućavanja ispravnog rada ili funkcioniranja uopće. Zanimljiv primjer dogodio se 2001. godine u Americi kada je trinaestogodišnji mladić onemogućavao ispravno funkcioniranje web stranice tvrtke Gibson Research Corporation (www.grc.com). Prijave FBI uredu, kao i davateljima Internet usluga su bile uzaludne jer se te organizacije tada nisu htjele iz različitih razloga pozabaviti ovim problemom. Vlasnik je osobno preuzeo inicijativu i otkrio kako se radi o navedenom mladiću koji je jedva znao što čini, a pogotovo nije bio u stanju razviti aplikacije potrebne za ovakve napade. Gotovo 500 računala sudjelovalo je u napadu na navedeni poslužitelj bez spoznaje svojih vlasnika, a količina zlonamjernih paketa koji su opterećivali poslužitelj približila se brojci od 20GB. Napadima je upravljano pomoću IRC poslužitelja, a kao trojanski konj korišten je alat Sub7Server koji je čak i automatizirano instalirao svoje nove inačice na zaraženom računalu te služio kao poslužitelj s kojeg su se izvodili napadi.

Iako je najčešće razlog zlonamjeran, napadi uskraćivanjem usluga nisu orijentirani prema stjecanju pristupa nedozvoljenim informacijama i podacima ili drugim sigurnosnim ili financijskim iskorištavanjima. Napadači DoS napade izvršavaju prvenstveno kako bi se međusobno dokazali ili kako bi nanijeli štetu napadnutim organizacijama. Iz tih napada oni nemaju nikakvu financijsku korist, ali napadnute organizacije često mogu imati velike štete. Štete se mjere u financijskim brojkama kao rezultat nemogućnosti poslovanja i potrebe za ulaganjem u sigurnosnu zaštitu, ali i u nefinancijskim mjerama pri čemu se prvenstveno misli na gubitak ugleda među klijentima i partnerima. Klijenti uslijed nemogućnosti korištenja standardnih usluga organizacije, iste traže kod drugih organizacija, a partneri gube povjerenje u napadnutu organizaciju.

Jedan od razloga za provođenje DoS napada je i prikrivanje nekih drugih zlonamjernih aktivnosti koje izvođači DoS napada paralelno izvode. Tako na primjer napadači mogu izvršiti DoS napad na računala koja prikupljaju log zapise ili detektiraju neovlaštene aktivnosti.

Da bi uzrokovali uvjete nedostupnih resursa, napadači mogu izvršiti različite oblike destruktivnih aktivnosti:

- rušenjem pojedinih aplikacijskih servisa (HTTP, električna pošta, itd.), napadači onemogućavaju legitimne korisnike u pristupanju istima,
- onemogućavanje pristupa pojedinim aplikacijskim servisima napadači mogu obaviti i postavljanjem izrazito velikog broja zahtjeva na ciljane servise čime poslužitelj nije u mogućnosti odgovoriti na sve upite ili su odgovori toliko spori pa se servis može proglasiti nefunkcionalnim,
- napadima na komunikacijske uređaje napadači mogu ili onemogućiti komunikacijski link ili ga usporiti na granicu neuporabljivosti,
- neovlaštenom izmjenom konfiguracijskih podataka napadači uzrokuju neispravno ponašanje servisa ili računala (npr. neovlaštenom promjenom tablica usmjeravanja na usmjerivačima, napadači uzrokuju nepravilno usmjeravanje mrežnih paketa), itd…

Od iznimne važnosti je napomenuti da se DoS napadi mogu dogoditi i spontano (nenamjerno), iako su rijetki. Konkretno, specifikacija nekog protokola može biti korektno izvedena, ali se tek dugotrajnim funkcioniranjem istog primijeti da kod npr. povećanog broja zahtjeva za nekim resursom, sustav bez razloga biva opterećen dulje nego je to potrebno. Rezultat je stanje onemogućenog korištenja resursa, ali nije uzrokovano osmišljenim napadom.

Napadi uskraćivanjem usluga najčešće se obavljaju od strane udaljenih napadača pa se globalno dijele na dvije skupine prema sloju odnosno nivou sedmo-slojnog OSI modela na kojeg su usmjereni. Na taj način moguće ih je podijeliti u dvije skupine:

- napadi usmjereni na aplikacijski sloj i

- napadi usmjereni na mrežne resurse, odnosno mrežni sloj.

Napadi na mrežne resurse često ne dolaze iz samo jednog izvora pa se takve naziva distribuiranim napadima uskraćivanja resursa (eng. DDoS - *Distributed DoS*). U narednim poglavljima raspoloživa je klasifikacija DoS napada u kojoj se nalazi podrobniji opis svakog od navedenih DoS napada.

3. DoS napadi na aplikacijskom sloju

DoS napadi na aplikacijskom sloju u većini slučajeva imaju za cilj onesposobljavanje i otežavanje rada računalnih aplikacija, a rjeđe i uzrokovanje trajnog prestanka rada računalnih servisa i aplikacija pri čemu mogu biti izvođeni od strane lokalnih ili udaljenih korisnika.

Glavni faktor koji pridonosi uspješnom provođenju aplikacijskih DoS napada je otežana metoda detektiranja od strane sustava za detekciju neovlaštenih aktivnosti (eng. IDS – *Intrusion Detection System*). Detekcija je otežana jer ove vrste napada ne zahtijevaju pojačan mrežni promet te takve pakete nije moguće razlikovati od uobičajenih paketa koji putuju mrežom. Aplikacijski DoS napadi pri radu koriste uska grla sustava te se koncentriraju upravo na ta aplikacijska ograničenja ne zahtijevajući pri tome korištenje pomoćnih sustava za izvore napada, kao što je slučaj s distribuiranim DoS napadima koji su objašnjeni u nastavku dokumenta. Stoga sustavi za detekciju neovlaštenih aktivnosti moraju biti prilagođeni različitim računalnim aplikacijama kako bi mogli detektirati neuobičajena ponašanja programa koja bi mogla rezultirati DoS stanjem.

Prilikom analize aplikacijskih DoS napada, postavlja se pitanje zašto su računalne aplikacije uopće ranjive na takve napade i mogu li se tijekom razvoja stvoriti aplikacije koje nisu podložne ovim napadima. Nažalost, odgovor na prethodno pitanje je negativan. Osnovni razlog propusta unutar aplikacija uzrokovani su kod razvoja i implementiranja zbog pogrešnih pretpostavki načinjenih u tim fazama razvoja. Također, programeri su često prisiljeni koristiti tuđe programe i programske biblioteke koje su neprovjerene i često sadrže različite nedostatke.

Tijekom razvoja aplikacija potrebno je imati na umu i namjenu njihovog korištenja. U skladu s tim, određuje se količina potrebne memorije, tipovi podataka, veličina polja te ostali programski elementi. Ukoliko se tijekom izvršavanja ili tijekom unosa korisničkih podataka, iz nekog razloga predviđeni kapaciteti premaše, rezultati su nepredvidivi i otvaraju mogućnost DoS napadima. Pogreške unutar aplikacije koje nisu izravno vezane za korisnički unos također se mogu iskoristiti za napade uskraćivanjem usluga.

Ukoliko se mogućnosti korisničkih unosa ne ograniče, zlonamjerni korisnici mogu unositi prevelike nizove ulaznih podataka koji mogu uzrokovati prepisivanje spremnika (eng. *buffer overflow*) te na taj način mogu onemogućiti daljnji rad ranjive aplikacije. I u slučajevima kada je aplikacija korištena kao sučelje između korisnika i nekog drugog programskog sustava poput baze podataka, uz nedovoljnu provjeru ulaznih podataka, moguće je obavljati različite zlonamjerne aktivnosti poput npr. nedozvoljenih SQL upita. Programeri često pretpostave kako će korisnici njihovih aplikacija biti samo ljudi, a ta pretpostavka nije ispravna. Korisnici mogu biti i drugi programi ili skripte koji vrlo lako mogu pretrpati ulaz podacima. Na primjer, često se koriste programi za tzv. „*brute force*“ napade koji između ostalog uključuju pogađanje zaporke korištenjem svih mogućih kombinacija znakova. Njihovim korištenjem napadači mogu maksimalno angažirati programe u obradi njihovih podataka čime ostali korisnici ne mogu dobiti kvalitetnu uslugu.

Najjednostavniji način izvršavanja DoS napada na aplikacije je na način da se iste koriste na način kako to nije zamišljeno. Klasični primjer je slanjem aplikaciji prevelikih količina podataka koje su puno veće nego što aplikacija u uobičajenom radu obrađuje. Takvo stanje može ili maksimalno okupirati aplikaciju pri čemu ista nije u stanju obraditi sve zahtjeve ili može trajno prekinuti njen rad.

Iskorištavanje različitih nedostataka aplikacije zasniva se na detaljnim analizama rada aplikacija, njenih funkcionalnosti te identifikacije i interpretacije unosa. Na taj način zlonamjerni korisnici mogu razotkriti različite nedostatke u radu aplikacije u svrhu uzrokovanja potpunog ili djelomičnog prestanka funkcioniranja napadnute aplikacije ili u svrhu uništavanja podataka kojima aplikacija u svom radu pristupa ili ih kreira.

3.1. Napadi preko korisničkih imena

Na velikom broju sustava, zlonamjerni korisnici su u mogućnosti pretrpavanja mehanizma autentikacije na način da se prijavljuju nerealno veliki broj puta. Na taj način zlonamjerni napadači mogu opteretiti mehanizam autentikacije i time djelomično ili potpuno onemogućiti prijavu drugih korisnika.

Zlonamjerni napadači pronalaze korisnička imena na različite načine. Ukoliko mehanizam prijavljivanja različito opisuje pogrešku uzrokovanu nepostojećim korisničkim imenom, a različito opisuje pogrešku uzrokovanu pogrešnom zaporkom, zlonamjernim napadačima olakšan je postupak detekcije legitimnih korisničkih imena. Stoga se od aplikacija zahtjeva prijavljivanje iste pogreške kako za neispravno korisničko ime, tako i za pogrešnu zaporku.
Sigurnost mehanizma prijave može se podići na višu razinu ako se određenom korisniku zabrani mogućnost prijave nakon određenog broja unosa netočnih zaporki. Ipak, i ta opcija posjeduje jedan veliki nedostatak. Naime, ako deblokiranje računa zahtijeva administratorsku intervenciju, zlonamjerni napadač može legitimnom korisniku ograničiti uslugu blokirajući njegov račun. Tu postoji mogućnost zabranjivanja ponovnog prijavljivanja s IP adrese s koje su detektirani neuspješni pokušaji, ali ta metoda može biti neefikasna jer se pomoću posrednih (eng. *proxy*) poslužitelja izvorište lako mijenja. Zbog svih prethodno navedenih razloga, najučinkovitija opcija je korištenje zaključavanja na određeni vremenski period nakon kojeg se korisnikov račun automatski otključa i biva osposobljen za korištenje.
Aplikacije koje zahtijevaju registraciju novih korisnika, podložne su napadima iscrpljivanja resursa ukoliko se proces registracije automatizira, a veliki broj registriranih korisnika se potom iskoristiti za različite oblike napada. Rješenje za ovaj potencijalni nedostatak je stvaranje niza izobličenih znakova te njihovo prikazivanje tijekom registracije u obliku slikovnog formata. Programi za optičko prepoznavanje znakova u nemogućnosti su prepoznati izobličene znakove te je na taj način spriječena automatska registracija korisnika. Drugi najčešće korišteni način je zasnovan na validaciji adrese elektroničke pošte, ali se i ova metoda može relativno jednostavno automatizirati pa stoga nije najbolja opcija.

3.2. Napadi orijentirani na transakcije

Svaka transakcija koju aplikacija napravi zahtjeva određeni interval procesorskog vremena i podatkovnog mjesta. Neke transakcije poput slanja SMS poruka putem Interneta imaju i financijske troškove. Napad uskraćivanja resursa je moguće izvršiti i obavljanjem velikih količina transakcija što može dovesti do onemogućenja uobičajenog rada aplikacije ili do većih financijskih troškova.

3.3. Napadi na baze podataka

Sustavi za upravljanje bazama podataka mogu biti procesorski vrlo zahtjevni ukoliko se radi o bazama s velikim količinama podataka ili kad se koriste posebno oblikovani upiti. Obzirom da web aplikacije sve češće koriste baze podataka za spremanje svojih podataka, napadi ovog tipa postaju nezanemarivi. Ukoliko napadač želi opteretiti žrtvinu vezu prema Internetu, napadač mora posjedovati bržu vezu od napadnute. Međutim, ukoliko postavi pažljivo osmišljen upit npr. pretrage u bazi podataka korištenjem regularnih izraza, napadač može napraviti mnogo veća opterećenja na sustav. Na taj način onemogućuje legitimnim korisnicima regularno korištenje baze podataka.

3.4. Napadi zasnovani na iscrpljivanju jedinstvenog identifikatora sjednice

Budući da HTTP protokol nije temeljen na stanjima, veze prema nekom poslužitelju nije moguće dovesti u odnos radi provjeravanja da li isti korisnik pristupa dvjema stranicama s poslužitelja. Stoga se svaki jedinstveni identifikator sjednice (eng. *session ID*) mora generirati prilikom prvog pristupa stranici, što oduzima procesorske resurse, i pohraniti nekamo, što oduzima podatkovni prostor. Napad se može izvršiti slanjem zahtjeva za velikim brojem jedinstvenih identifikatora sjednica što će na različite načine iscrpiti resurse, a time će se onemogućiti rad ostalim korisnicima. Ovakav napad je moguć samo ako aplikacija generira taj broj prije autentikacije. Ukoliko se najprije zahtijeva autentikacija, mogućnost ovih napada je smanjena jer se korisnik može samo jednom prijaviti. Ipak, ako je dozvoljeno više sjednica po jednom korisniku, tada je aplikacija i dalje ranjiva. Najsigurnije rješenje za ove vrste napada je dozvoljavanje jedne sjednice po korisniku te onemogućavanje automatskih registracija novih korisnika što je pojašnjeno prethodnim poglavljima.

3.5. Napadi zasnovani na prepisivanju spremnika

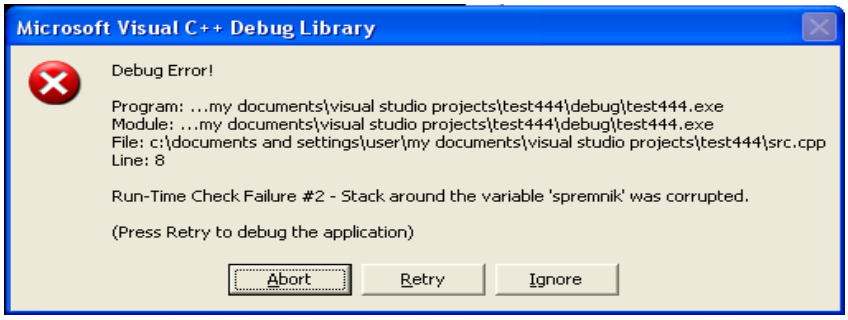
Kako je već objašnjeno, funkcioniranje aplikacije uvelike ovisi o predviđanjima programera na temelju kojih je aplikacija razvijana. Najčešće se pogreške događaju kod upravljanja memorijom i zauzimanja iste i to kod jezika koji zahtijevaju takav pristup, kao što su npr. C i C++. Jednostavan

programski isječak koji dovodi do pogreške prepisivanja spremnika (eng. *buffer overflow*) u jeziku C može se vidjeti na sljedećem primjeru.

```
void prepisivanje(char *niz) {
   char spremnik[10];          /* Zauzimanje memorije */
   strcpy(spremnik, niz);      /* Opasna funkcija  kojom se
                                  parametar niz nepoznate
                                  veličine kopira u spremnik
                                  fiksne veličine */
}

int main() {
  char *niz = "Ovaj niz sigurno sadrži više od 10 znakova!";
  prepisivanje(niz);
  return EXIT_SUCCESS;
}
```

Pogreška izazvana ovim programskim kodom uzrokuje stvaranje datoteke sa sadržajem memorije na dijelu gdje je došlo do pogreške i prekid izvršavanja programa. Na Windows platformama pogreška izaziva upozorenje vidljivo na sljedećoj slici:



Slika 1: Prijava pogreške prepisivanja spremnika kod izvođenja aplikacije

Primjerom prikazana pogreška može se lako izbjeći pažljivijim razvojem aplikacije, ali kod dinamičkih unosa kod web aplikacija vjerojatnost pojave pogrešaka prepisivanja spremnika višestruko se povećava. Korištenje programskih jezika višeg nivoa poput Java, PHP ili C# onemogućuje kontrolu na nižem nivou, ali i onemogućuje pogreške ovog tipa. Zlonamjerni korisnik može uočavanjem ovakvih propusta vrlo jednostavno uzrokovati stanje uskraćivanja aplikacijskih usluga.

3.6. Napadi zasnovani na nemogućnosti otpuštanja zauzetih objekata ili resursa

Najčešća pogreška ovog tipa je kod programskih jezika gdje se zauzeti objekti moraju eksplicitno osloboditi od strane programera. Kod C/C++ jezika to se uglavnom događa sa zauzetom memorijom koja se ne oslobodi nakon regularnog završetka programa, a pogotovo nakon neregularnog završetka. To dovodi do tzv. curenja memorije (eng. *memory leak*). Kod jezika poput Jave često se ne predvide svi mogući završetci izvođenja programa pa resursi poput veza na bazu podataka ostaju zauzeti i po završetku programa, a nakon određenog broja stvorenih i nezatvorenih veza, rad s bazom podataka postaje otežan te konačno i onemogućen. Ukoliko napadač uoči pogreške ovog tipa, vrlo lako ih može izazvati i time uzrokovati stanje nepravilnog funkcioniranja sustava.

3.7. Napadi zasnovani na prevelikim zahtjevima napadača

Ukoliko se korisniku omogući izravan ili neizravan unos podataka bez dovoljne provjere, a isti se podaci koriste kao uvjet programske petlje, aplikaciju se može smatrati podložnom DoS napadima. Pretpostavi li se rad s aplikacijom koja ispisuje informacije o određenom broju osoba pri čemu korisnik definira broj korisnika o kojima će biti ispisane informacije, korisnik tu lako može otežati rad aplikacije. Na primjer, unosom broja koji doseže najveću vrijednost cjelobrojne 32 bitne varijable,

sigurno će doći do velikog usporenja sustava, zauzeća memorije, opterećenja sustava za upravljanje bazama podataka i sl. Stoga je uvijek potrebno ograničiti mogućnost korisničkih unosa, pogotovo kada oni izravno utječu na izvršavanje programa.

3.8. Napadi zasnovani na kreiranju programskih objekata

Jednostavan programski kod poput narednog primjera pokazuje način na koji se može korisniku omogućiti stvaranje proizvoljnog broja novih objekata.

```
String TotalObjects = request.getParameter("numberofobjects");
int NumOfObjects = Integer.parseInt(TotalObjects);
ComplexObject[] anArray = new ComplexObject[NumOfObjects];  // opasno!
```

Posljednja linija instancira u polju `anArray` onoliko objekata koliko iznosi parametar `NumOfObjects`. Upravo iz tog razloga brojni programski jezici ne dozvoljavaju instanciranje polja ugrađenih tipova ili objekata koristeći varijable, nego samo koristeći konstante, vrijednosti koje se nužno programski definiraju i korisnik ih ne može mijenjati.

3.9. Napadi na sistemske dnevničke zapise

Različiti programi koriste dnevničke (eng. *log*) zapise kako bi zabilježili svoje aktivnosti. Uzrokujući velik broj dugih zapisa u log datotekama, moguće je popuniti diskovni prostor. Primjerice, poslužitelj koji bilježi sve nadolazeće zahtjeve može biti meta automatiziranog napada dugim zahtjevima. Rješenje za ovaj oblik DoS napada nalazi se u pažljivom određivanju podataka prilikom osmišljavanja i implementacije aplikacije, kako se ne bi omogućio upis ogromnim količinama podataka i tako ostvarili povoljni uvjeti za izvršavanje DoS napada.

3.10. Napadi korištenjem elektroničke pošte

Najjednostavniji oblik napada na pretince elektroničke pošte sastoji se od odašiljanja velikih količina elektroničkih poruka na ciljnu adresu. Efektivne DoS napade moguće je izvesti i postavljanjem lažne izvorne adrese poruke elektroničke pošte. Primjerice, postavljanje poruke na *usenet* grupe pri čemu se koristi tuđa adresa, uzrokovat će dolazak neželjenih *spam* poruka na žrtvinu adresu, a ovisno o sadržaju, moguće su i poruke od legitimnih korisnika koji nemaju saznanja da se radi o prijevari. Rješenje se može naći u ograničavanju odašiljanja poruka elektroničke pošte s neistinitom adresom. Odašiljanje velikog broja poruka na nepostojeće adrese, pri čemu je porukama lažirana izvorna adresa, uzrokovat će velik broj prijava nemogućnosti isporuke tih poruka, ali na adresu koja je upisana kao izvorna – žrtvina adresa. Jedan od mogućih napada na nečiju adresu elektroničke pošte jest prijavljivanje te adrese za primanje obavijesti pojedinih stranica, ali taj napad se lako spriječi zahtijevanjem validacije dane adrese.

4. DoS napadi na mrežnom sloju

Cilj DoS napada na mrežnom sloju je onemogućavanje ispravnog funkcioniranja mrežnih usluga i komunikacijskih kanala. Navedeno je moguće postići na dva načina:

- pretrpavajući komunikacijske kanale (eng. *flooding attacks*) i
- iskorištavanjem ranjivosti mrežnih usluga i protokola (eng. *vulnerability attacks*).

Napadi su uglavnom usmjereni na zauzeće komunikacijskog kanala i onemogućavanja uspostave veze pa su to napadi koji za cilj imaju pretrpavanje računalnih i mrežnih resursa. Drugi najčešći tip su napadi koji iskorištavaju ranjivosti u mrežnim uslugama.

Napadi pretrpavanjem komunikacijskog kanala izvode se slanjem velike količine podataka na mrežu što uzrokuje nemogućnost normalnog prenošenja legitimnih podataka. Odašiljanje velike količine zahtjeva za uspostavom veze onemogućit će rad računalnim resursima i računalo više neće biti u mogućnosti obrađivati legitimne zahtjeve niti uspostaviti vezu s legitimnim korisnikom. Pri tome napadači uobičajeno lažiraju izvorne IP adrese ili ignoriraju odgovore.

Najjednostavniji oblik napada, s obzirom na broj računala uključenih u napad, jest situacija u kojoj se napad izvodi s jednog računala, a odredište je također jedno računalo. Efektivnije mogućnosti zasnovane su na korištenju više računala kao izvora napada, pri čemu jedno računalo predstavlja

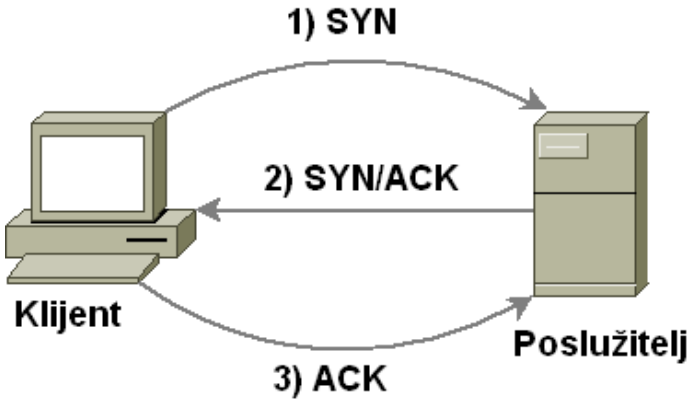
žrtvu. Međutim, napadi iz više izvora na više ciljeva, kao ni napadi na više ciljeva iz jednog izvora, nisu rijetkost.

4.1. Napadi korištenjem posebno oblikovanih mrežnih paketa

Opis napada zasnovanih na posebnom oblikovanju mrežnih paketa pretpostavlja poznavanje važnijih mrežnih protokola i pojmova vezanih uz njih. U ovom dokumentu pojašnjeni su samo najznačajniji pojmovi.

TCP (eng. *Transmission Control Protocol*) označava protokol koji određuje način komuniciranja između računala. Protokol je zadužen za uspostavu, održavanje i prekid veze. Uspostavljanje veze korištenjem TCP protokola naziva se „*Three-Way Handshake*“, a odvija se postavljanjem odgovarajućih zastavica (eng. *flag*) u mrežnim paketima. Uloga zastavica upravo je određivanje sadržaja i tipa paketa. Primjerice, zastavica SYN (eng. *synchronize*) koristi se kod uspostave veze, ACK (eng. *acknowledge*) se koristi kao potvrda za primljeni paket, a zastavica FIN (eng. *finish*) se koristi za prekid uspostavljene veze.

Uspostava veze odvija se na način da klijent pošalje poslužitelju paket s postavljenom zastavicom SYN. Ukoliko poslužitelj može uspostaviti vezu s klijentom, poslužitelj mu vraća paket s postavljenim SYN i ACK zastavicama kao potvrdu o otvaranju veze s njegove strane. Ako pak nije u mogućnosti uspostaviti vezu, vraća ICMP paket ili paket s postavljenim RST (eng. *reset*) i ACK zastavicama. Konačno, kada klijent primi paket sa SYN/ACK zastavicama, odgovara paketom s postavljenom ACK zastavicom i razmjena podataka može početi. Grafički je uspostavljanje veze između klijenta i poslužitelja prikazano na slici *Slika 2*, a prikaz mrežnog prometa analiziran alatom Ethereal dan je na slici *Slika 3*.



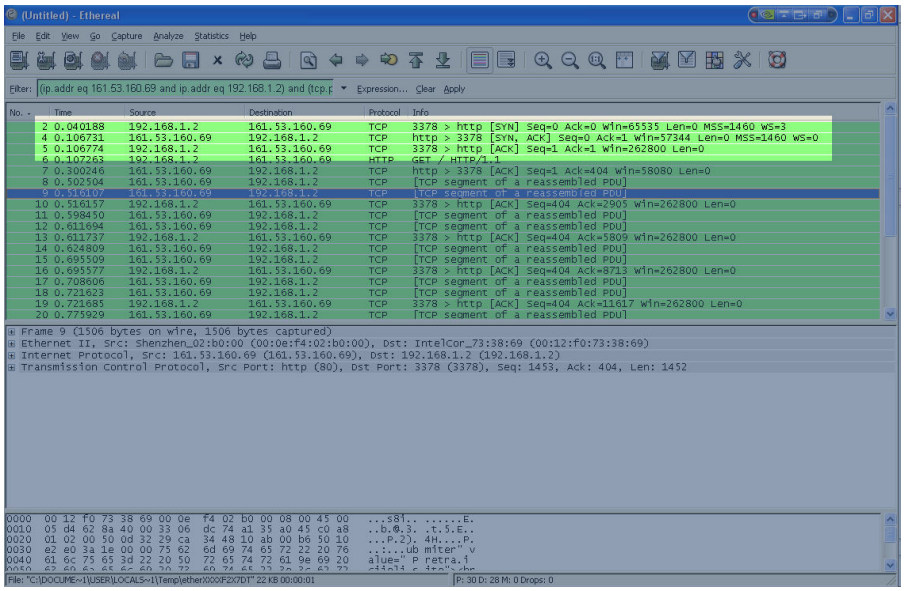
Slika 2: Uspostava veze kroz tri koraka

4.1.1. Napadi pretrpavanja paketima s postavljenom SYN zastavicom

Primanjem paketa s postavljenom SYN zastavicom, poslužitelj je upozoren na stvaranje nove veze prema njemu. Pripremanje za prihvat nove veze obuhvaća alokaciju memorijskog prostora za primanje i slanje podataka te za podatke vezane uz opis veze. Poslužitelj potom odašilje klijentu SYN/ACK paket i čeka na odgovor. Na taj način je poslužitelj spreman za primanje klijentskog ACK paketa i za razmjenu podataka. Ukoliko ne primi odgovor u nekom roku, poslužitelj ponovno odašilje SYN/ACK paket smatrajući kako se prethodni izgubio na putu do odredišta. Upravo je ova činjenica omogućila napade pretrpavanja poslužitelja paketima s postavljenom SYN zastavicom i lažnom izvornom IP adresom. Ukoliko lažna adresa nije dodijeljena niti jednom računalu na Internetu, poslužitelj odašilje SYN/ACK paket na nepostojeću adresu čekajući odgovor koji nikad neće dobit. Resursi napadnutog računala nisu beskonačni i nakon dovoljne količine takvih zahtjeva, poslužitelju je onemogućeno normalno funkcioniranje i odgovaranje na legitimne zahtjeve. Ukoliko je pak lažna izvorna adresa slučajno odabrana i to tako da postoji računalo na Internetu kojemu je dodijeljena, tada će to računalo poslati napadnutom poslužitelju paket s postavljenom RST zastavicom i na taj način dati mu do znanja da ono nije zatražilo uspostavu veze.

Ne postoji jednostavan način za pronalaženje izvora ovih napada jer im je izvorna adresa lažna. Obrana se može temeljiti na detektiranju povećanog broja primljenih SYN paketa. U tom slučaju se stvaraju privremene datoteke na računalu unutar kojih se bilježe podaci o mogućim uspostavama veza,

a datoteke se nazivaju SYN-kolačićima (eng. *SYN-cookie*). Ukoliko se primi odgovarajući ACK paket, alociraju se potrebni resursi za omogućavanje nove veze. Drugo rješenje je konfiguriranje vatrozida kao tzv. *SYN-proxy* poslužitelja. Tada vatrozid umjesto poslužitelja zaprima veze i tek kada je veza uspješno uspostavljena, vatrozid prosljeđuje zahtjeve poslužitelju simulirajući proces uspostave veze u tri koraka.



Slika 3: Uspostava TCP veze s www.cert.hr u tri koraka

4.1.2. Napadi pretrpavanja otvorenim vezama

Napad izvorno izvođen korištenjem Naptha alata, samo je proširenje napada pretrpavanjem SYN paketima. Izvorna zamisao je ostvariti što veći broj uspostavljenih veza prema napadnutom sustavu, najčešće je riječ o web poslužiteljima, kako bi ih onemogućili u ispravnom funkcioniranju. Cilj ostvarivanja velikog broja uspješno otvorenih veza je iscrpljivanje ograničenog broja mrežnih priključaka (eng. *socket*) na napadnutom računalu. Obrana se temelji na brojanju otvorenih veza i ograničavanju količine uspješno ostvarenih veza u sekundi. Drugi način za obranu ne postoji, jer je količina mrežnog prometa generirana ovim napadima vrlo mala i veza se uspostavlja na potpuno ispravan način.

4.1.3. Napadi pretrpavanja paketima s postavljenom ACK zastavicom

Iz navedene procedure uspostavljanja veze u tri koraka moguće je iskoristiti još jedan način napada, a to je generiranjem paketa s postavljenom ACK zastavicom. Napadnuto računalo dodijelit će određeno procesorsko vrijeme obradi pristiglog paketa, kako bi na posljetku ustanovilo da se radi o paketu koji nije namijenjen njemu, odnosno kojemu nije prethodio SYN paket. Velika količina primljenih paketa onemogućit će ispravno funkcioniranje računala.

4.1.4. Napadi pretrpavanja ICMP paketima

U slučaju kada velika količina ICMP paketa, tipa *ECHO REQUEST*, optereti poslužitelj zahtijevajući povratne odgovore, resursi napadnutog sustava se u određenom trenutku opterete u tolikoj mjeri da nisu u mogućnosti zadovoljiti pristigle legitimne mrežne pakete. Ukoliko se napadačevo računalo nalazi na sporijoj vezi nego je napadnuto računalo te ukoliko se napad izvede na pogrešan način, mogući ishod napada može biti pretrpavanje računala zlonamjernog korisnika velikim količinama ICMP odgovora. Jedno od mogućih rješenja nalazi se u ograničavanju broja ICMP paketa u jedinici vremena pri čemu se svi ostali odbacuju kada je prag prijeđen. Također, moguće je i u potpunosti zabraniti ICMP pakete na ulazu u mrežni segment. Ovakvi napadi često se izvršavaju na DNS poslužitelje kako bi onemogućili legitimne korisnike u pristupu željenim odredištima preko naziva tih odredišta (web, ftp, …).

4.1.5. Napadi pretrpavanja UDP paketima

UDP (eng. *User Datagram Protocol*) je izvorno zamišljen i implementiran kao protokol koji ne zahtijeva prethodnu uspostavu veze između dviju točaka Interneta kako bi mogao prenositi podatke. Stoga ovakvim napadima nije moguće jednostavno izvoditi pretrpavanje paketima koje bi onemogućilo stabilan rad sustava. Međutim, usmjeravanje paketa na nepostojeću (slučajno generiranu) pristupnu točku (port), uzrokuje od strane odredišnog sustava provjeru postoji li neka usluga koja je otvorila taj port. Ukoliko ne postoji, napadnuti sustav odgovara ICMP paketom kako ne može dosegnuti traženi port. Paket odgovora usmjeren je na adresu pročitanu iz zahtjeva. Ukoliko je ona lažna, paket će nakon nekog vremena biti odbačen. Dovoljno velika količina ovakvih paketa ne samo da može onemogućiti napadnuto računalu u izvršavanju uobičajenih funkcija, nego je moguća i situacija u kojoj će se i količina prometa mrežom drastično povećati te će se otežati legitimno prometovanje mrežom.

4.1.6. *Smurf* napadi

Smurf napad je jedan od DoS napada koji je svoje ime dobio po aplikaciji koja izvršava ovaj tip napada. Riječ je o stvaranju *ECHO REQUEST* paketa s lažnom izvornom adresom te odašiljanju istog usmjerenog na sva računala unutar mrežnog segmenta, koristeći tzv. *broadcast* adresu. Razlog korištenja navedene adrese kao ciljne jest što takav paket zahtjeva biva isporučen svim računalima u mreži, a to pridonosi pojačanju intenziteta napada odnosno količine paketa koji kolaju mrežom pa se ti napadi često nazivaju napadima pojačavanja (eng. *amplification attacks*). Ishod je velika količina ICMP paketa odgovora usmjerenih na žrtvino računalo i velika količina prometa na mrežnom segmentu. Obrana od *Smurf* napada se sastoji od pravilnog konfiguriranja usmjerivača na mreži: onemogućavanjem *broadcast* usmjeravanja ili podešavanjem vatrozida da ne propušta *ECHO REQUEST* pakete. Izbjegavanje primanja velike količine paket odgovora lako se može izvesti nepropuštanjem *ECHO REPLY* paketa ili ograničavanjem njihovog broja u odnosu na ukupan broj paketa koji prometuju mrežom po jedinici vremena. Odabrano računalo koje je dio mreže i koje je navedeno kao izvor ICMP zahtjeva ne može utjecati ni na koji način u sprječavanju ovih napada.
Na stranicama http://www.powertech.no/smurf/ moguće je izvršiti provjeru ranjivosti na ovaj tip napada.

4.1.7. *Fraggle* napadi

Ideja *Fraggle* napada preuzeta je od *Smurf* napada, ali za razliku od *Smurf* napada koji koriste ICMP pakete, *Fraggle* koristi UDP pakete. UDP paketi se pri tome šalju na *broadcast* adresu mreže. Uklanjanje ovog napada je otežano jer korištenje UDP protokola često nije moguće zabraniti kao što je slučaj s ICMP protokolom. UDP se često koristi kod različitih aplikacija koje ne traže potvrdu o prijenosu već prvenstveno traže brz prijenos. Stoga nije moguće efikasno koristiti niti metode obrane zasnovane na ograničavanju brzine propuštanja UDP mrežnih paketa.

4.1.8. *Targa3* napadi

Targa3 napadi se zasnivaju na oblikovanju neispravnih paketa bilo kojeg protokola. Izvorno su zamišljeni za izvođenje napada na računala s Windows operacijskim sustavima, ali su se kasnije počeli primjenjivati i za ostale operacijske sustave. Ukoliko posebno oblikovani paket stigne na odredište, operacijski sustav alocira potrebnu količinu memorije i ostalih resursa za njegovu obradu, a u konačnici je posao uzaludan jer paket nikad i nije bio ispravan. Danas vrlo malo ovakvih paketa uopće dosegne odredište jer bivaju odbačeni već pri odlasku od ISP-a (eng. *Internet Service Provider*).

4.1.9. Napadi fragmentacijom paketa

Svaka poruka koju je potrebno prenijeti komunikacijskim kanalima Interneta, ukoliko prelazi podrazumijevanu maksimalnu veličinu, dijeli se u manje pakete. Ti manji paketi ne moraju doći na odredište pravilnim redoslijedom jer je to dozvoljeno od strane definicije protokola. Napadi zasnovani na fragmentaciji paketa koriste upravo tu osobinu razdjeljivanja poruke u više paketa pri čemu paketi ne moraju doći pravilnim redoslijedom.
Između ostalih, jedan od poznatijih napada zasnovan na fragmentaciji napada naziva se *Rose* napadom. Ovim napadom se stvaraju samo prvi i zadnji paket. Ranjivi sustav očekuje i ostale pakete pa rezervira resurse za obradu i postavlja se u stanje čekanja. Ukoliko su svi resursi u tom stanju, niti

jedan legitiman zahtjev neće biti obrađen. Ciljni port pri tome uopće nije važan jer se prikupljanje paketa radi na nižoj razini od one na kojoj se radi interpretacija njegova sadržaja. Slično vrijedi za izvornu IP adresu čijim se lažiranjem može samo dodatno otežati detektiranje izvora napada.
New Dawn napad se zasniva na prethodno opisanom *Rose* napadu, ali radi se o nešto složenijoj izvedbi. Fragmenti se generiraju počevši od prvog do zadnjeg, ali uz manji broj propuštenih dijelova poruke. Računalo koje prima takav nepotpuni slijed paketa alocira dovoljno mjesta za čitavu poruku, ali ju nikada ne primi u potpunosti. Ishod napada je povećano korištenje resursa sustava na štetu legitimnih zadataka koje sustav obavlja.
Starije inačice operacijskih sustava imale su prilično loše implementacije sklapanja primljenih paketa u izvornu poruku pa se često ovim napadima moglo uzrokovati prestanak rada sustava ili ponovno pokretanje istog (*Teardrop* napad).
Moguće rješenje za suzbijanje napada zasnovanih na fragmentaciji paketa, nalazi se u ograničavanju vremena tijekom kojeg se čeka dok nepotpuni niz paketa bude odbačen te u ograničavanju broja ponovljenih zahtjeva za odašiljanjem neprimljenih paketa. Novije implementacije sastavljanja poruke iz paketa ne rezerviraju unaprijed memoriju nego pridošle pakete spremaju u vezanu listu sve dok ne pristignu svi koji čine poruku.
Ostale varijante ovih napada su *SYNdrop*, *Boink*, *Nestea Bonk*, *TearDrop2* i *NewTear*.

4.1.10. *Ping of Death* napad

Jedan od poznatijih DoS napada je *Ping of Death*. Pretpostavljena veličina ICMP paketa jest 56 okteta. Starije inačice operacijskih sustava poput Mac OS i Windows 95 nisu bile u stanju obraditi ICMP *echo* pakete veće od 1024 okteta. Primitak ovakvih paketa je kod Windows 95 operacijskih sustava uzrokovao pojavu tzv. *Blue Screen of Death* (BSoD), plavog ekrana s prijavom nemogućnosti nastavka rada. Jedan od načina obrane od ovih napada je zasnovan na nedozvoljavanju prolaska ICMP *echo* (tip 8) paketa na vatrozidu. Međutim, kada je to postao učestao način obrade, napadači su se dosjetili odašiljanju *echo reply* paketa te su na taj način zaobilazili obranu i uspješno pretrpavali računala nepotrebnim i beskorisnim podacima. Ipak, danas svi operacijski sustavi posjeduju zaštitu od ovog oblika napada.

4.1.11. *Land* napadi

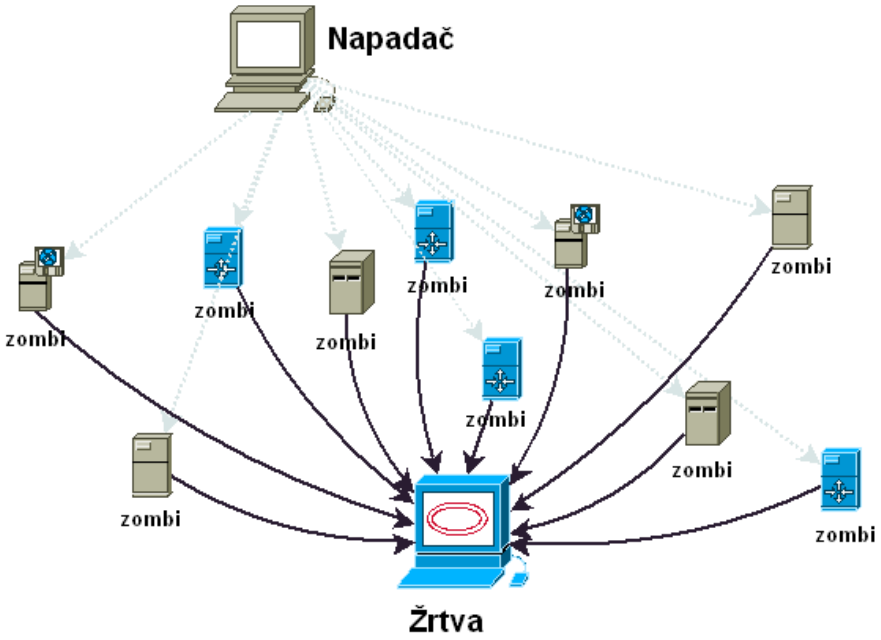
Ukoliko napadač pošalje paket s istom ciljnom i izvornom IP adresom radi se o *Land* napadu. Operacijski sustavi koji bi primili ovakav paket, najčešće su prestajali s radom i automatski bi se resetirali. Također, moguće je i uzrokovanje kontinuirane međusobne razmjene paketa između dva odredišta. Obrana od ovih napada nije jednostavna kao što bi se u prvi mah zaključilo. Obrana se sastoji od pravilne konfiguracije vatrozida koja sprečava dolazak ovakvog paketa do sustava kojem je namijenjen.

4.2. Raspodijeljeni napadi

Raspodijeljeni napadi su oni napadi koji su zasnovani na korištenju više računala kao izvora napada, pri čemu jedno računalo predstavlja žrtvu. Napadač pri tome može na određeni način preuzeti kontrolu nad posrednim računalima, ali to nije nužno. Detaljni opis raspoloživ je u nastavku ovog poglavlja.

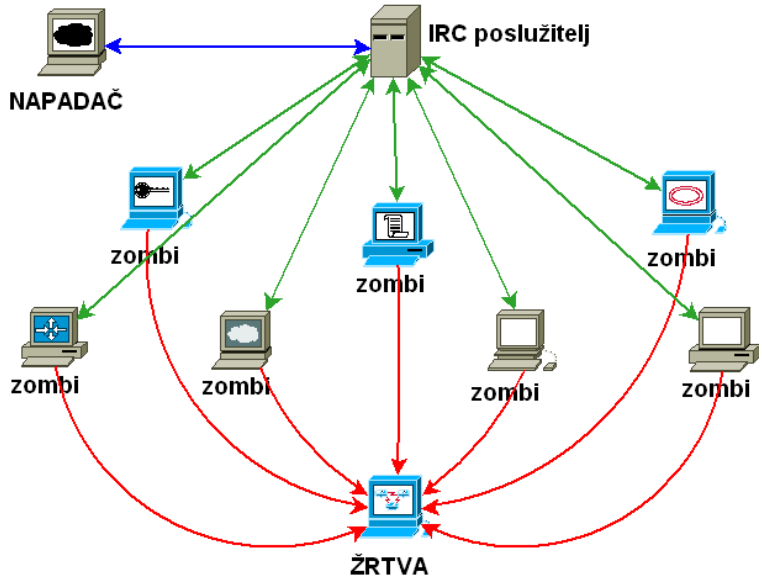
4.2.1. DDoS napadi

DDoS (eng. *Distributed DoS*) su napadi izvršeni od strane raspodijeljenih napadača, odnosno većeg broja napadača. Najčešće su to računala zvana zombijima (eng. *zombie*) čiji vlasnici nisu upoznati s činjenicom da njihovo računalo generira DoS napade na neko računalo ili računala na Internetu. Na ovaj način je moguće stvarati velike količine prometa na napadnutim mrežnim segmentima čiji dio jest i napadnuto računalo ili mrežni uređaj. Cijela ideja je prikazana na sljedećoj slici.



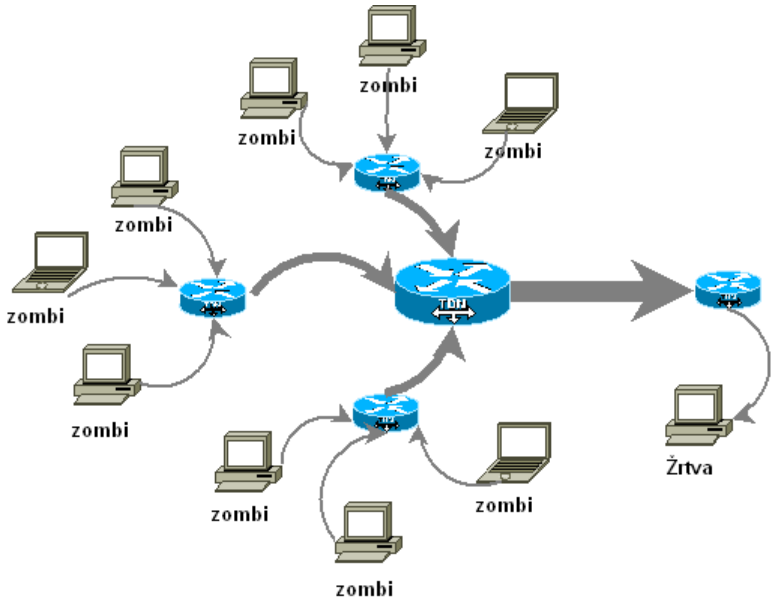
Slika 4: Zombi računala kontrolirana od strane napadača

Raspodijeljeni napadi nisu namijenjeni aplikacijskom sloju iz jednostavnog razloga što je za napade na aplikacije dovoljno iskoristiti ranjivosti istih, a za to nije potrebna veća količina mrežnog prometa. Ideja ostvarena ovim napadima je ispunjavanje komunikacijskih kanala beskorisnim prometom koji onemogućuje prometovanje legitimnih mrežnih paketa te iskorištavanje velikih količina resursa poslužitelja, računala korisnika i dugih mrežnih uređaja. Navedeno se realizira stjecanjem kontrole nad računalima korisnika Interneta kako bi ih se iskoristilo u svrhu stvaranja mrežnog prometa. Neki od poznatih alata korišteni za izvršavanje DDoS napada su MyDoom, Sub7Server, Trin00, Stacheldraht i TFN (*Tribe flood network*). Na slici *Slika 5* prikazan je načelan rad napada uz korištenje Sub7Server alata na zombi računalima pri korištenju IRC poslužitelja kao poveznice između napadača i zlonamjernog alata.



Slika 5: Korištenje IRC poslužitelja kao veze između napadača i izvođača napada (zombi računala)

Slika 6 prikazuje odnose količina prometa generiranih DDoS napadima te primjenu na napadnuto računalo odnosno usmjerivač kojim je napadnuto računalo povezano na Internet. Na slici je debljina strelica između pojedinih računala i usmjerivača proporcionalna količini mrežnog prometa između njih.



Slika 6: Količine mrežnog prometa na pojedinim segmentima

Iz slike *Slika 6* je očito kako velike količine prometa s Interneta dolaze do usmjerivača mreže kojoj pripada žrtva. Svi oni paketi koji ne budu bili proslijeđeni u bilo kojem smjeru, biti će odbačeni. U navedeno su uključeni i legitimni paketi što dovodi napadnutu mrežu u stanje neispravnog funkcioniranja.

SYN, ACK i *Fragment* napadi, opisani u prethodnim poglavljima, izvode se korištenjem raspodijeljenih izvora te na taj način stvaraju mnogo veće količine prometa nego bi to mogao samo jedan napadač čak i uz veliku brzinu veze prema Internetu.

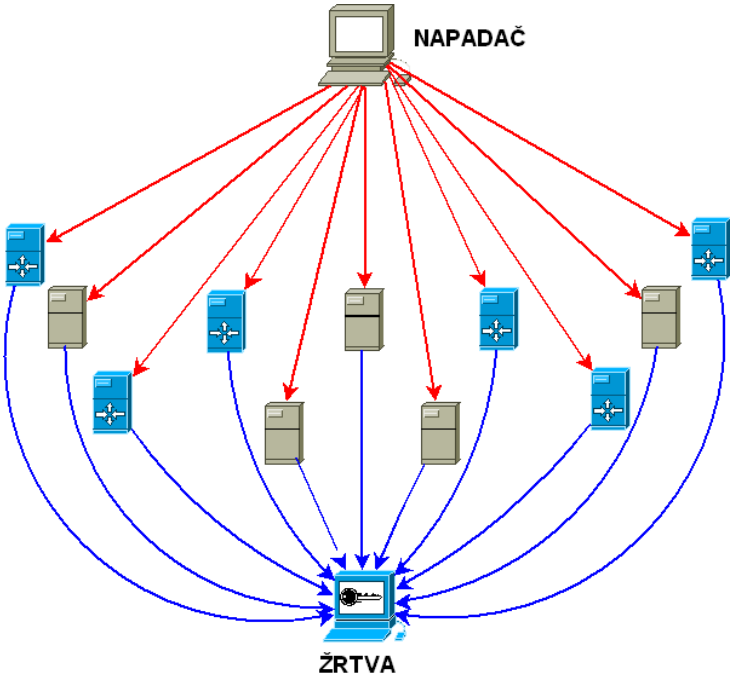
Napadi mogu uključivati i slanje poruka elektroničke pošte na jednu ili više adresa (navedeno kod napada na aplikacijskom sloju), a tada im najčešće nije potrebna kontrola napadača. Primjer su brojni crvi (eng. *worm*) koji se šire različitim načinima i odašilju poruke elektroničke pošte nekom specifičnom korisniku ili češće svim korisnicima nađenim pretraživanjem primljenih poruka i adresara. Na ovaj način ne samo da je generiran neželjen skup elektroničkih poruka nego je i povećan promet Internetom zbog potrebe za isporukom istih.

Problemu raspodijeljenih napada mogli bi ISP uređaji stati na kraj ukoliko bi vodili računa o prometu koga stvaraju njihovi korisnici. Nažalost, najčešće oni to ne čine. Ovisno o vrsti napada mogu se stvoriti filtri na usmjerivačima koji povezuju napadnuti mrežni segment i Internet. Zadatak tih filtra bio bi odbacivanja neželjenog prometa koji mu pristiže s Interneta i namijenjen je nekom računalu na njegovoj mreži. Pravilna konfiguracija vatrozida, korištenje antivirusnih aplikacija na korisničkim računalima (potencijalnim zombijima) i izbjegavanje javnog objavljivanja adrese elektroničke pošte, koraci su koji mogu spriječiti ili barem umanjiti ishode napada.

Na napad se može početi sumnjati već pri prvim pojavama usporenja mrežnog prometa, nedostupnosti nekog web sjedišta (stranice), nemogućnosti pristupa bilo kojoj web stranici i sl.

4.2.2. DRDoS napadi

DRDoS (eng. *Distributed Reflection DoS*) napadi su vrlo slični DDoS napadima prema učinku na kranju žrtvu i količinu generiranog prometa. Razlika ipak postoji i vrlo je važna. Na slici *Slika 7* je grafički prikazana shema ovih napada za slučaj jednog napadača.



Slika 7: Shema izvršavanja DRDoS napada

DRDoS napadi se zasnivaju na uspostavi veze u tri koraka. Napadač (ili skupina napadača) stvara TCP paket s postavljenom SYN zastavicom kako bi inicirao vezu prema nekom postojećem računalu na Internetu. Međutim, paket je tako oblikovan da je na mjesto izvorne adrese postavljena IP adresa žrtve. SYN paket dospijeva na odredište, a ono odgovara na adresu iz izvorišnog polja. Ukoliko poslužitelj može uspostaviti vezu, paket s postavljenim SYN i ACK zastavicama biva odaslan prema žrtvi. Jednako tako moguće je za odašiljanje ICMP paketa koristiti potpuno istu logiku. Tada će *ECHO REPLY* paketi zatrpavati žrtvu. Razlog uspjeha ovih napada se nalazi u tomu što se ne generira veća količina podataka na pojedinim posrednim računalima od kojih se odbijaju paketi pa nema nikakve sumnje u odvijanje napada. Privremeno rješenje u slučaju napada bila bi izmjena IP adrese žrtve ukoliko se radi o poslužitelju i promjeni odgovarajućih zapisa u DNS poslužiteljima. Moguće je i postaviti filtriranje na odgovarajućim usmjerivačima ukoliko dolazni paketi imaju neko zajedničko svojstvo. Ukoliko je napad privremeni i jednokratni isplati se i povećati resurse i odolijevati napadu dok ne prestane iako to nije optimalno rješenje. Najbolja opcija je pripremiti se za napade unaprijed ukoliko se radi o važnoj usluzi koja mora biti neprekidno dostupna, rezervirati rang IP adresa kako bi se relativno brzo nakon detektiranja napada moglo prijeći na korištenje novih adresa i sl.

5. Zaštita od DoS napada

Ovisno o tomu na koji su sloj napadi usmjereni, moguće je u manjoj ili većoj mjeri utjecati na njihovo suzbijanje. Budući da se različiti oblici uskraćivanja usluga u okviru istog sloja ne zasnivaju na istim tehnikama i ranjivostima, nije ih moguće spriječiti ili umanjiti na jedinstven način. Za optimalnu obranu potrebno je napraviti što jasniju podjelu istih i tražiti rješenja za onemogućavanje pojedinih, te načine obrane podijeliti u što jednostavnije cjeline. Kao u i ostalim životnim sferama, prevencija je najjednostavniji i najlakši način obrane od DoS napada s najmanje posljedica. Međutim, obzirom da nije moguće predvidjeti sve oblike DoS napada, u ovom poglavlju su obrađeni i tehnički načini sprečavanja ili umanjivanja ishoda u situacijama kada su napadi u tijeku.

Kao što je već spomenuto prethodno u dokumentu, DoS napadi na aplikacijskoj razini mogu biti izrazito teški za uočavanje, a time i za sprečavanje. Razlog tomu je nemogućnost razlikovanja mrežnih paketa sa zlonamjernim sadržajem u odnosu na pakete s legitimnim sadržajem. Obrana od ove vrste napada mora se temeljiti na nekim drugim metodama, prvenstveno na redovitoj primjeni zakrpa i instalaciji odgovarajućih nadogradnji.

Načini obrana na mrežnom sloju mogu se analizirati pažljivom podjelom svih potrebnih aktivnosti, a takav pristup opisan je u nastavku ovog poglavlja. Ovi napadi su mnogo lakše uočljivi od napada na

aplikacijskoj razini jer uglavnom uključuju povećane količine mrežnog prometa, neuobičajene mrežne pakete i sl.
Naputci za uspješnu obranu od DoS napada:

- pravilno konfigurirati vatrozid,
- primijeniti odgovarajuće zakrpe za obranu od napada pretrpavanjem SYN paketima,
- onemogućiti nepotrebne i nekorištene servise,
- omogućiti ograničenja diskovnog prostora za pojedine korisnike,
- napraviti procjenu legitimnog korištenja resursa za lakšu detekciju napada,
- redovno provjeravati fizičku ispravnost svih resursa,
- koristiti alate za detekciju izmjena konfiguracijskih datoteka,
- investirati u kupovinu i izgradnju pomoćnih uređaja koji bi se koristili tijekom napada,
- investirati u sigurnu izgradnju mrežne infrastrukture kako bi se povećala tolerancija na pogreške,
- redovito izrađivati sigurnosne kopije sustava ili njihovih najvažnijih dijelova,
- pažljivo osmisliti načine dodjele zaporki, dozvola i sl.

5.1. Prevencijske strategije

5.1.1. Pripreme za napad

Vrlo često se smatra kako se loše stvari događaju drugim ljudima ili organizacijama te se zaštiti od različitih napada ne posvećuje dovoljna pozornost. Često odgovorne osobe posvećuju dovoljnu pažnju sigurnosti računalnih resursa tek nakon što ih pogode određeni oblici računalnih napada. Ovakav pristup obrani od DoS napada u potpunosti je pogrešan. Osim mogućih visokih troškova za organizacije, jedan od razloga zašto je prevencija važna je i jednostavnost izvođenja DoS napada pa iste danas mogu izvoditi i djeca koja malo više vremena provode na Internetu. Bez planiranja unaprijed, razmjeri napada mogu biti jako veliki. Za slučaj napada potrebno je imati pripremljene procedure, odnosno načine reakcije kada napad započne te pripremljene dovoljne količine ljudskih i tehnoloških resursa koji se mogu dovesti u stanje potpunog funkcioniranja u vrlo kratkom roku.

5.1.2. Procjena usluga koje bi mogle biti metom napada

Za efikasnu obranu potrebno je odrediti usluge koje pripadaju najrizičnijoj kategoriji i za koje je najveća vjerojatnost da će biti metom DoS napada. U organizacijama se uglavnom koristi ista veza prema Internetu za odlazni i dolazni web promet, primanje i slanje poruka elektroničke pošte, DNS upita, povezivanje podružnica organizacije kod neke specifične usluge poput baza podataka, te za razne druge usluge. U slučaju odvijanja napada, npr. pretrpavanjem porukama elektroničke pošte, istodobno će i sve ostale usluge pretrpjeti posljedice nepravilnog funkcioniranja računalne mreže. Stoga je potrebno odrediti prioritete pojedinih usluga kako bi im se u izvanrednim okolnostima mogla dati dozvola za korištenje preostalih funkcionalnih resursa.

5.1.3. Suradnja s davateljem Internet usluga

O suradnji s davateljima Internet usluga (ISP) ovisi uspjeh u obrani od nekih napada zasnovanih na uskraćivanju usluga. Naime, s obzirom da su mrežni uređaji poput usmjerivača koji su u posjedu ISP-a bliže izvoru napada nego je žrtva, tada bi oni mogli biti točka obrane od nadolazećeg zlonamjernog prometa mrežom te na taj način spriječiti dolazak istog do žrtve kojoj je prvenstveno i namijenjen. Najčešće su te tvrtke pripremljene za većinu mogućih napada pa ih se može primijeniti kao primjer u osmišljavanju procedura za obranu na korisnikovoj strani. Naime, napadi na korisnika u velikoj se mjeri tiču njegovog davatelja Internet usluga jer time opterećuju i ostali legitimni promet.

5.1.4. Organiziranje rezervnih resursa

U trenutku kada napad započne sva sredstva moraju biti dostupna i pripravna za uporabu. Povećanje propusnosti komunikacijskih kanala, postavljanje zamjenskog poslužitelja za upravljanje prometom i slične aktivnosti moraju biti poduzete u što kraćem roku.

5.1.5. Postupci u slučaju napada

Jasno i suvislo definirani postupci u slučaju napada moraju postojati kod davatelja Internet usluga i kod krajnjeg korisnika – potencijalne žrtve. ISP može osigurati pomoć u osmišljavanju postupaka koji će se izvršavati u trenucima napada. Tehnička služba korisnika treba biti svjesna odgovornosti koja je pred nju postavljena u vezi obrane, ali i u postupcima prijave napada davatelju usluga. Kod raspodijeljenih napada najčešće izvori stvaranja zlonamjernih paketa pripadaju većem broju organizacija koje posjeduju pojedine mrežne segmente pa je i te organizacije potrebno kontaktirati i upozoriti na događanja. Dodatno, moguće je prijaviti policiji napad ili pokušaj napada te im prepustiti odgovornost nalaženja krivca.

5.1.6. Osiguranje

Kada je dostupnost usluge važna za poslovanje tvrtke ili organizacije, moguće je sklopiti ugovor s osiguravajućom tvrtkom koja bi u slučaju napada isplaćivala ugovorene naknade. Naravno, osiguravajuće tvrtke pri tome mogu zahtijevati od organizacije primjenu određenih oblika zaštite od računalnih napada.

5.2. Tehničke strategije

5.2.1. Detekcija napada

Napade na mrežnom sloju može se otkriti na različite načine što ovisi o vrsti napada. Napadi koji se temelje na posebnom oblikovanju mrežnih paketa ili na neuobičajenom protokolu, prilično se jednostavno otkriju. Mnogo teže je uočiti napade koji simuliraju način pristupa legitimnih korisnika, primjerice, ponavljajući zahtjeve za uspostavom veze. Također, velike količine poruka elektroničke pošte stvorene s namjerom zagušenja mrežnog prometa, često je nemoguće razlikovati od legitimnih poruka.

Razumijevanje ponašanja legitimnog korisnika i mrežnog prometa stvorenog na taj način temelj je na komu se zasniva identifikacija prometa generiranog od strane izvođača napada. Za takvu se namjenu koriste sustavi za detekciju napada (IDS) i alati za nadzor mrežnog prometa koji mogu prepoznati anomalije u prometu i poslati upozorenje odgovarajućem osoblju. U slučaju kada se napadi na temelju sadržaja paketa ne mogu razlikovati od legitimnog mrežnog prometa, potrebno je osigurati da mehanizmi detekcije napada analiziraju količine podataka ili broj veza po klijentu ili slično.

Sekundarne nadzorne procedure moraju biti u stanju prepoznati napade ukoliko primarne ne uspiju. Tu pripadaju različite skripte koje periodički provjeravaju dostupnost usluge ili web stranice i sl. Od velikog je značaja zapisivanje analiziranog prometa u dnevničke datoteke kako bi se omogućila i kasnija analiza te osigurali dokazi.

5.2.2. Filtriranje mrežnog prometa na usmjerivačima

Nepotreban mrežni promet bi trebao biti odbačen već na usmjerivačima kako ne bi uzalud iskorištavao resurse mrežnih segmenata kojima nije potreban niti namijenjen. Na primjer, mehanizam koji onemogućuje pretrpavanje paketima s postavljenom SYN zastavicom bi trebao biti implementiran na uređaju koji se nalazi na ulazu paketa u mrežni segment krajnjeg korisnika, tj. na vatrozidu. Postoje komercijalna rješenja za ovaj slučaj, ali ukoliko se popuni komunikacijski kanal između korisnika i davatelja Internet usluga, tada uređaji nisu od koristi nego je potrebna suradnja ISP-a u ublažavanju ili onemogućavanju napada. Mrežni uređaji namijenjeni detektiranju i odbacivanju ilegalnih paketa zahtijevaju mnogo procesorske snage i memorijskih resursa, pogotovu u slučaju napada, o čemu treba voditi računa kod instalacije odnosno izgradnje takvih uređaja. Iz istog razloga poželjno je da se vatrozid nalazi na ulazu u mrežni segment davatelja Internet usluga.

5.2.3. Ograničavanje prolaska paketa kod davatelja Internet usluga

Najbolja opcija za odbacivanje neželjenih paketa je već na ulazu u mrežni segment organizacije koja omogućava Internet usluge, kao što je već opisano. Jedan od razloga tomu je dovoljno velika širina komunikacijskog kanala i manja udaljenost od napadača. Filtriranje može biti temeljeno na:

- izvornoj i ciljnoj IP adresi mrežnog prometa i
- vrsti mrežnog prometa.

Ukoliko se radi o jednoj izvornoj adresi za sve dolazeće pakete, odbacivanje temeljeno na ciljnoj i izvornoj adresi je jednostavan proces. U slučaju raspodijeljenog napada (DDoS), organizacija koja daje Internet usluge mora u dogovoru s organizacijama koje posjeduju izvorne mreže blokirati promet koji dolazi s njihovih mrežnih segmenata. Dakako, pitanje je ostvarivosti ovakvog čina jer se na taj način i legitimnim korisnicima onemogućuje pristup pa je moguće da bi takav potez učinio više štete nego koristi.

Davatelji Internet usluga mogu izvršiti odbacivanje mrežnog prometa temeljeno na vrsti prometa. To im omogućuje odbacivanje i propuštanje samo određenih tipova mrežnih paketa. Kada su određene usluge od velikog značaja za krajnjeg korisnika, ISP može dati veći prioritet njima, a pri tome onemogućiti neke manje važne ili odgoditi vrijeme isporuke paketa namijenjenih uslugama s manjim prioritetom.

5.2.4. Segmentacija mrežnog prometa

Kada su identificirane ključne usluge, moguće je razdijeliti iste od onih koje su manje značajne. Ukoliko je, primjerice, dostupnost web stranica ključna za posao, treba razmisliti o poslužitelju na brzoj vezi u posjedu ISP-a. Usluge manjeg značaja, poput elektroničke pošte i FTP poslužitelja mogu biti posluživane i na računalima klijenta. Kod osmišljavanja obrane od različitih oblika DoS napada, potrebno je uočiti usko grlo u sveukupnom sustavu na koje će se napadač najvjerojatnije koncentrirati. Ako je moguće, za sekundarne DNS poslužitelje i poslužitelje elektroničke pošte trebalo bi odabrati računalo domaćin koje je dio nekog drugog mrežnog segmenta odnosno davatelja Internet usluga.

5.2.5. Obrana od napada koji su u tijeku

Kada sustav postane žrtvom napada, jedno od najjednostavnijih rješenja za obranu jest izmjena IP adrese napadnutog računala ako se radi o jednom napadnutom računalu. Zapisi u DNS poslužitelju jednostavno se ažuriraju i time ciljna adresa gomile zlonamjernih mrežnih paketa biva nepostojeća, a oni odbačeni. Ukoliko postoji mogućnost, dobar način obrane bio bi privremeno povećanje resursa i kapaciteta komunikacijskih kanala kako bi napad u što manjoj mjeri utjecao na legitiman promet. Dakako, spomenuta solucija nije odgovarajuća za učestale napade, ali kao privremeno rješenje ju svakako treba razmotriti.

Najjednostavnija obrana zasigurno bi bila isključivanje sve opreme s Interneta odnosno uzrokovanje potpune nedostupnosti usluga. Metoda najčešće nije izvediva, ali u iznimnim slučajevima može se primijeniti.

6. Zaključak

Današnji korisnici Interneta su takvi da je, na žalost, potrebno ulagati velike napore u istraživanje Internet sigurnosti i postavljanja odgovarajućih restrikcija kako zlonamjerni korisnici ne bi postigli uspjeh u onemogućavanju rada legitimnih korisnika. Velik dio napada čine i DoS napadi kako na aplikacijskoj razini, tako i na mrežnoj. Izvođenjem DoS napada napadači mogu uzrokovati velike financijske i ostale štete. Činjenica je da su DoS napadi, prisutni u sve većem broju i većim razmjerima, vrlo često izvođeni od strane neupućenih korisnika koji uopće ne razumiju funkcioniranje istih, a često ne shvaćaju niti razmjere problema koje su uzrokovali. S druge strane, prisutni su i drugi duboko upućeni poznavatelji Internet protokola i načina njegova funkcioniranja, koji razvijaju alate namijenjene zlonamjernom korištenju iz različitih razloga.

Dok postoje zlonamjerni korisnici, a uvijek će ih biti, potrebno je razvijati i pomno pripremati obrane od najrazličitijih mogućih napada. Rastom broja korisnika Interneta i povećanjem složenosti njegovih sastavnih dijelova, povećava se i broj potencijalnih napada i njihovi razmjeri. Područje sigurnosti na Internetu sve češća je tema, a njome se bavi sve veći dio stručnjaka iz računalnog svijeta.

7. Reference

[1] Stephen de Vries, A Corsaire White Paper: Application Denial of Service (DoS) Attacks, veljača 2004.

[2] Stephen de Vries, A Corsaire White Paper: Surviving Distributed Denial of Service (DDoS) Attacks, veljača 2004.

[3] Randal Vaughn, Gadi Evron, DNS Amplification Attacks, ožujak 2006.

[4] Distributed Reflection Denial of Service, http://www.grc.com/dos/drdos.htm, lipanj 2006.

[5] Computer Crime Research Center, Network security: DoS vs DDoS attacks, http://www.crime-research.org/articles/network-security-dos-ddos-attacks, prosinac 2006.

[6] Abhishek Singh, Demystifying Denial-Of-Service attacks, http://www.securityfocus.com/infocus/1853, prosinac 2005.

[7] CERT® Coordination Center, Denial of Service Attacks, http://www.cert.org/tech_tips/denial_of_service.html, travanj 2001.