Obrana sustava

Iako obrambeni mehanizmi ne prate razvoj DoS tehnika, uz adekvatno izgrađenu mrežnu strukturu i ispravno namještene mrežne uređaje moguće se efektivno obraniti od većine DoS napada. Dakako apsolutna zaštita od DoS napada ne postoji zbog same prirode Interneta, već postoje samo bolje ili lošije osigurani sustavi. U sljedećim poglavljima su obrađene neke od ideja i tehnika obranete njihove utjecaje na napade.

Generalna Strategija

Obrambene strategijesegrade u ovisnosti o vrsti napada.Nisu sve jednako uspješne u svakoj prigodi, stoga treba pomno analizirati i proučavati napade. Testiranje i traženje slabe točke u sustavu je jedan od najboljih načina zaštite.Može se generalizirati da se proces DoS obrane sastoji od ovih koraka:

1. Priprema. Nužno je razumjeti kako radi mreža sustava kojeg se želi zaštititi. Do razumijevanja se dolazi pretraživanjem i analizom. Bitno je znati topologiju mreže i nalaziti mjesta gdje može doći do zagušenja.
2. Detekcija. Ako je jedini način detekcije napada pad sustava, većina manjih napada će ostati neprimijećena iako i ti napadi mogu puno reći o ranjivosti sustava i namjerama napadača. Stoga je ključno primijetiti što više nelegalnih radnji unutar mreže i proučiti iste. U primjeni se to obavlja s zapisivanjem (eng. logging) dnevnika podataka i tehnikama detekcije upada u sustav (eng. Intrusion Detection Systems, IDS)
3. Karakterizacija. Koristeći pakete prikupljene u detekciji, te konzultacijom s drugim izvorima podataka zaključujemo o kojoj se vrsti napada radi. Kako nije potreban velik broj paketa da se očita vrsta napada, druga potrebna stavka karakterizacije je i otkrivanje otkud dolaze paketi. Često nije moguće doći do samog napadača praćenjem veza, ali je moguće dobiti dojam o pozicijama njegove botnet mreže. Razmjenom takvih informacija među napadnutim organizacijama može se približiti izvoru napada i uhvatiti napadača uz potporu institucija pravde.
4. Reakcija. S obzirom na vrstu napada postupa se da bi se minimalizirala šteta ili spriječio napad. Koristeći blokiranje prometa, smanjenje alociranih resursa prema određenim vezama i slične akcije smanjuje se opterećenost sustava i potencijalno onemogućava uspješnost napada. Dobro je imati postavljene procedure napravljene za specifične vrste napada.
5. Analiza. Postmortem analizom dobivamo ključne informacije o obrani našeg sustava, te pregledom podataka možemo locirati ranjive točke. Lokacijom ranjivih točki možemo ispraviti greške unutar sustava i unaprijediti obranu istog.

Tehnike

SYN Cookies

SYN kolačići su ključan element obrane od SYN Flood napada. Tehniku su predstavili 1996. Daniel J. Bernsteina i Eric Schenk. Cilj ove zaštite je osloboditi 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.

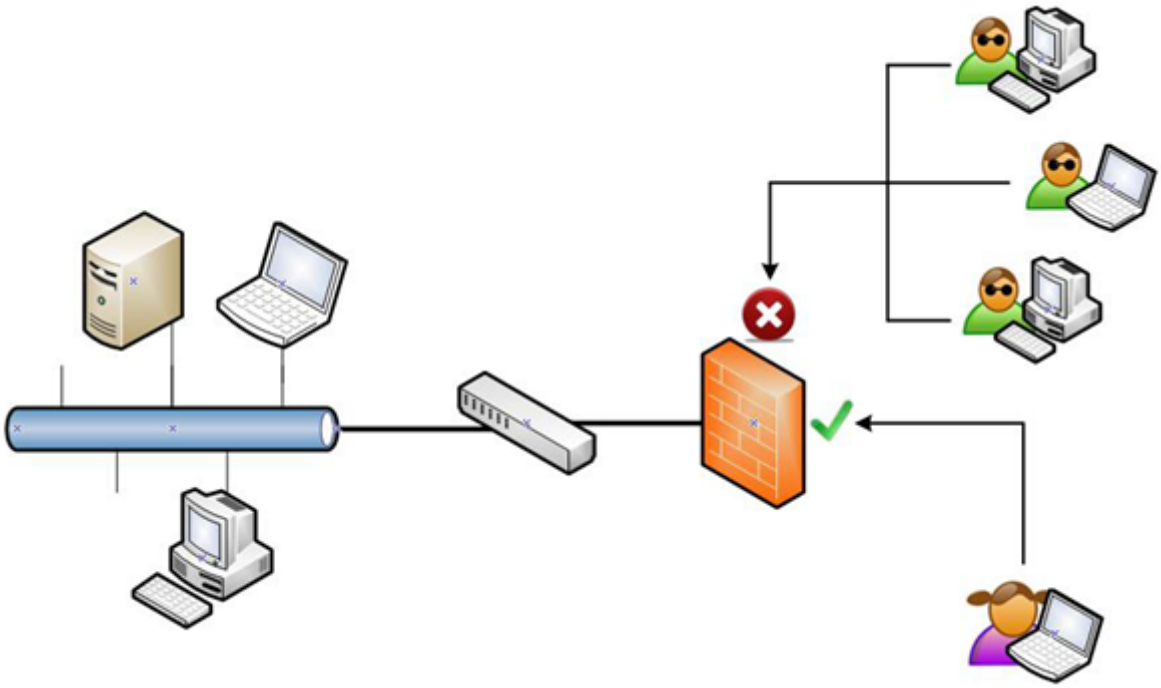
Tek ukoliko poslužitelj dobije nazad ACK od klijenta on alocira resurse i u potpunosti uspostavlja vezu. Implementira se tako štoprilikom slanja SYN-ACK paketa poslužitelj u slijedni broj kodira informaciju potrebnu za rekonstrukciju pristiglog SYN paketa. Jednom kada klijent pošalje ACK paket, poslužitelj će iz kodirane informacije 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. Linux jezgra (eng. kernel) podržava implementaciju SYN kolačića od siječnja 1997. Naravno, ovaj oblik zaštite ima svoja ograničenja. Sam poslužitelj troši resurse za prihvat i slanje poruka, te tako postoji resursni limit i pored opterećenja koje se oduzima primjenom SYN kolačića. Da bi se unaprijedio sustav SYN kolačića napravljen je noviji standard TCP Cookie Transactions (TCPCT).

TCPCT

TCPCT je nadogradnja TCP protokola zamišljena da ga osigura od SYN flood napada slično kao i SYN kolačići. Za razliku od SYN kolačića koji su podržani u strukturi TCP-a, TCPCT mora biti podržan od strane primatelja i pošiljatelja da bi se mogao implementirati kao ekstenzija TCP-a. 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. Ovakvim radom ne opterećuje se poslužitelj zauzimanjem resursa sve dok se ne završi three-way handshake. Dodatno, ovakvim sustavom je implementirano da poslužitelj odmah otpušta resurse po prekidu veze, što nije slučaj u običnoj implementaciji TCP-a. TCPCT je djelomično integriran u Linux jezgru verzije 2.6.33 (prosinac 2009.)

Hardverska zaštita

Primjenom dediciranih mrežnih uređaja za filtriranje i regulaciju prometa u mreži može se postići znatno smanjenje učinkovitosti DoS napada na sustav. Različiti mrežni uređaji kao što su vatrozid (Firewall), preklopnik (switch), usmjerivač (router) ili IPS (Intrusion prevention systems) imaju različite mogućnosti ograničavanja ili smanjivanja utjecaja DoS napada. Prilikom implementacije mreže svakako je potrebno iskoristiti te mogućnosti. Pravilnom konfiguracijom vatrozida može se podesiti niz pravila koja dopuštaju ili zabranjuju određene pakete da uđu u lokalnu mrežu.Moguće je definirati maksimalnu protočnost podatkovne veze teograničiti 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.

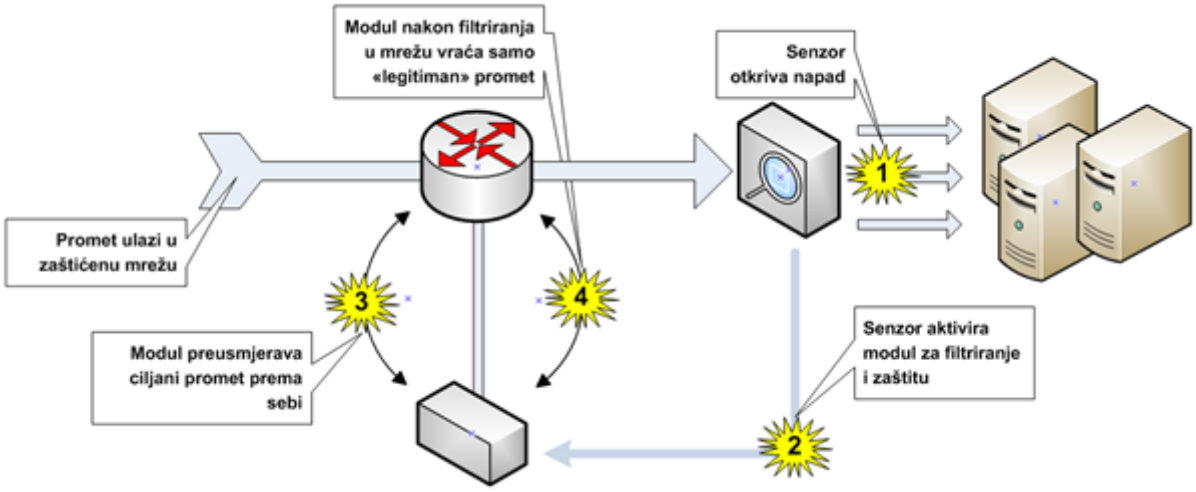


Napredniji uređaji

Iako dobra konfiguracija osnovnih uređaja daje puno veću razinu zaštite nego nepripremljen sustav, ovi uređaji ne mogu pružati savršenu zaštitu. Primarno zato što nisu dizajnirani samo s tom svrhom na umu. Za bolju zaštitu treba posegnuti za naprednijim uređajima. Neki od tih uređaja su:

- Filtar prometa -uređaj koji preusmjerava dolazni promet prema mreži i provodi filtriranje .
- Senzor -uređaj koji prati promet na ključnim točkama u mreži i obavještava modul za filtriranje i zaštitu o pojavi napada.

Primjer jedne mreže s ukomponiranim filtrom i senzorom možemo vidjeti na slici u nastavku.



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.