Distributed Denial-of-Service (DDoS) Attack - og hvordan man forsvarer sig imod det

Bo Lindhøj
Artavazd Hakhverdyan

May 21, 2012

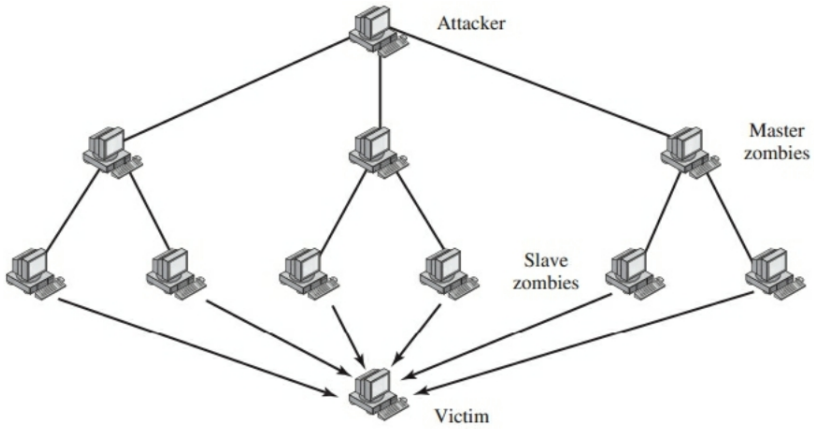
Contents

1 Introduktion

I denne rapport vil vi fokusere på de såkaldte Distributed Denial-of-Service (DDoS) angreb. DDoS angreb udgør en trussel mod internettets stabilitet. Selv store virksomheder som Yahoo!, eBay og Amazon.com bliver udsat for DDoS angreb. Cyber gangstere kan med DDoS angreb afpresse virksomheder som er afhængige af en stabil internetforbindelse. Vi vil starte med at beskrive hvad et DDoS er og hvordan man kan forsvare sig imod dem. Derudover vil vi beskrive det forsvarssystem som bliver introduceret i artikelen 'Defending against Flooding-Based Distributed Denial-of-Service: A Tutorial' af Rocky K. C. Chang.

2 Hvad er et DDoS angreb?

Et DDoS angreb er et forsøg på at forhindre en host i at udføre den service som den er sat i verden for at udføre. Det gøres typisk ved at en angriber sender mange ubrugelige angrebs pakker mod et offer. Pakkerne kommer fra en række kompromitterede hosts. Offeret bliver dermed overbelastet således at forespørgsler til og fra hosten bliver meget langsomme og i praksis umulige. Offeret kan være én computer, en server eller et helt netværk. Angrebs pakker kan være TCP, ICMP, UDP, eller en blanding af dem. Der findes to generelle typer for DDoS angreb, direkte og indirekte angreb.



(a) Direct DDoS Attack

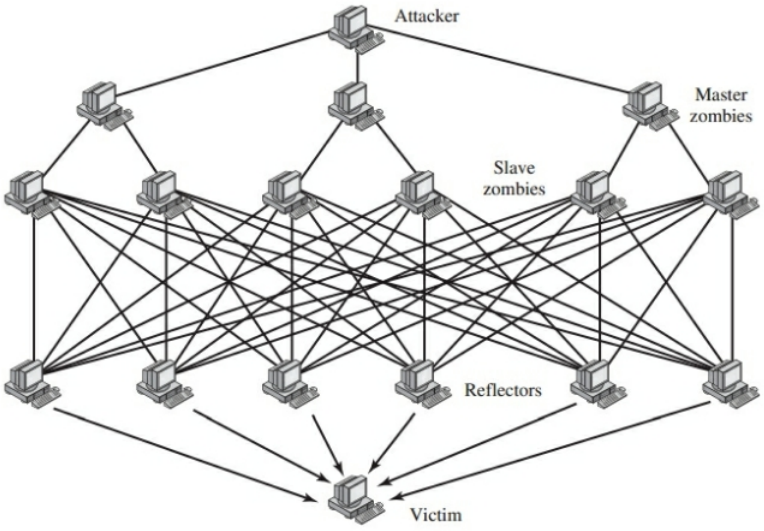
2.1 Direkte angreb

I et direkte DDoS angreb sender angriberen en masse angrebs pakker direkte til offeret. Før et angreb kan finde sted er angriberen nødt til at skabe DDoS angrebs netværk. Han sidder ved en host og kompromitterer en række andre hosts. Disse hosts kan så hver især kompromittere yderligere flere hosts. Dem der direkte er komprimerede af angriberen kaldes master zombies og dem der er kompromitterede af master zombies kaldes slave zombies. Pakkerne der ankommer til offeret har spoofede IP'er. Hvis det er TCP, er det typisk et SYN

flooding angreb, hvor der bruges et stort antal TCP SYN pakker der bliver sendt til offerets server port. Da pakkerne har spoofede IP'er, bliver responsen sendt et andet sted på internettet. Så offeret sender flere SYN-ACK pakker før den giver op. Disse halvåbne forbindelser vil efterhånden udgøre alle serverens mulige forbindelser og dermed gør det umulige for nye forbindelser at finde sted. De DDoS angreb man kender i dag kan angribe flere ofre ad gangen. Figuren på side 3 viser netværket i en direkte angreb.

2.2 Reflector (indirekte) angreb

I et Reflector angreb bruges visse hosts (reflectors) i angrebet uden at være kompromitterede. Angriberen sender pakker til reflektorerne der kræver tilbagesvar, men i pakkerne står offerets adresse som kildeadresse. Enhver protokol der understøtter "automatisk besked generering" kan bruges til reflector angreb heriblandt TCP og UDP pakker og diverse ICMP beskeder. Når der bliver brugt TCP angrebs pakker kan en reflector svare med enten SYN-ACK pakker (til SYN pakker) eller RST pakker (til uægte TCP pakker). Udover ICMP echo beskeder kan mange ICMP fejlbeskeder bruges i et reflector angreb. Eksempelvis vil angrebspakker, indskrevet med inaktive destinationsporte, udløse hosts til at sende 'ICMP port utilgængelig'-beskeder. Netværket i et reflector angreb ligner meget netværket for direkte angreb, men her er der et ekstra lag af mange reflecterer. Følgende figur viser netværket i et reflector angreb.



3 Forsvarssystem mod DDoS

Man kan groft set kategorisere forsvarsmekanismerne til et DDoS angreb i tre kategorier. Forebyggelse, man vil gerne sørge for at DDoS angrebet ikke finder sted. Detektion og filtrering, de ting man kan gøre når man er under angreb. Identifikation, når angrebet har fundet sted vil man gerne finde ud af hvor det kommer fra, så man evt. kan finde angriberen.

3.1 Forebyggelse

Under forebyggelse kan man inddele det i yderligere to kategorier, passiv og aktiv forebyggelse. Passiv forebyggelse går ud på at man sikrer sig at ens maskiner, ikke bliver overtaget og gjort til zombier. Der findes kendte port scannings metoder som man skal sikre sig imod, samt man kan sørge for at have installeret de seneste sikkerhedsopdateringer til diverse services. En anden passiv metode er at overvåge den trafik der er på netværket, og lede efter kendte pakker der sendes mellem en master og og en slave zombie. En aktiv måde hvorpå man kan forebygge DDoS angreb, er at have cyber spioner, der kigger på diverse fora, for at se om et evt DDoS angreb er under opsejling.

3.2 Detektering og Filtrering

Hvis et DDoS angreb finder sted, vil man gerne være i stand til at detektere det, så man kan iværksætte evt. modforanstaltninger. Den første del er detekteringen, den står for at finde ud af hvornår man er under angreb og hvilke pakker der er angrebs pakker. Dernæst er det filtreringens opgave at klassificere og droppe angrebs pakkerne, så systemet kan opretholde sin service. Detektion og filtrering når man er under angreb, kan pga. den distribuerede natur af angrebet, kun bruge sine egne informationer IP, adresser, til at finde angrebs flows. Den overordnede succes afhænger af både detektion og filtrering. En metode til at måle for god detektion man har, er at se på false positive og false negative ratios. False positive ratio er givet antal pakker klassificerede som angrebs pakker/ antal bekræftede normale pakker. False negative ratio er givet som antal angrebspakker klassificerede som normale/antal bekrfætede angrebspakker. Under et angreb vil man gerne have disse så tæt på nul som muligt, for ikke at fejl klassificerer pakker. En måleenhed for hvor god filtrering er, at se på normal packet survival ratio (NPSR), den procentdel af normale pakker der når sit mål. Hvis man under angreb pga. false positive komme til at fejl klassificere og dermed droppe normale pakker, vil dette også nedsætte systemets service. En effektiv filtrerings mål, under et angreb, er at have et så højt NPSR som muligt. Detektion og filtrering kan umiddelbart placeres 4 steder på netværket, som ses af følgende figur. Som det ses af pilene på billedet vil detektering være

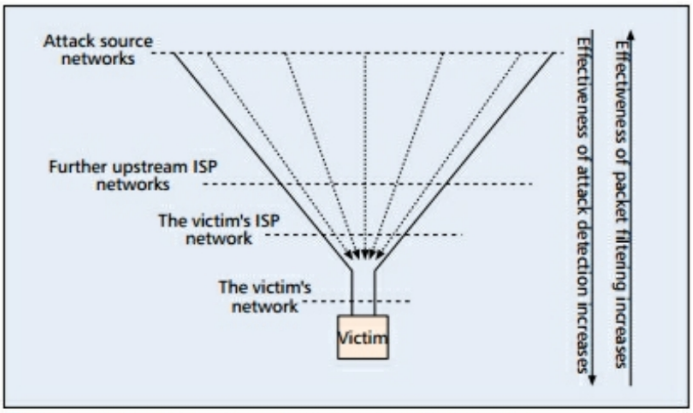


Figure 4. *Possible locations for performing DDoS attack detection and filtering.*

lettere nu tættere det er placeret på offeret, da de fleste pakker tæt på offeret er til offeret. På offerets netværk har man mulighed for at overskue alle pakkerne, og genkende angrebs mønstre. Hvorimod der langt oppe i netværket vil være mange andre pakker, der ikke er tiltænkt offeret, og derfor er ligegyldige. Filtrering derimod er mere effektivt nu længere væk fra offeret det finder sted. Her kan for eksempel bruges et Ingress filter, der kontrollere at kilde og destinations adresserne er gyldige og droppe pakker med ugyldige informationer. Tæt på offeret er de fleste pakker til offeret, og der vil derfor også blive droppet normale pakker, hvilket er uønskværdigt.

3.3 Identifikation

Denne fase finder sted efter at man er blevet ramt af et DDoS angreb. I denne fase vil man gerne forsøge at lave et traceback og finde ud af hvem der har udført angrebet. Denne fase kan ikke udføres mens angrebet finder sted, da ens netværk er lammet. Hvis man under angrebet fandt ud af hvem der udførte, ville det alligevel være meget svært at stoppe dem. Derfor er denne fase mest til efterfølgende at gå lovens vej og fange en evt. angriber. En måde at lave traceback på, er ved at få routerne i netværket til at gemme informationer om hvorfra de har modtaget en pakke. På den måde kan man backtracke tilbage til hvor bakken er kommet fra, ind i netværket. En anden måde er at få routerne til at tilføje mere information til pakkerne, så man kan se hvilken vej de er kommet af, eller ved hjælp af ICMP. Hvis angrebet har været et indirekte reflector angreb, så er IP traceback stort set umuligt, da pakkerne kommer fra reelle kilder, og ikke direkte fra angriberen.

4 En distribueret løsning "Internet Firewall"

Da der ikke findes global forsvarsmekanisme mod DDoS angreb bliver der i artiklen foreslået at indføre en "internet firewall" til at beskytte hele internettet mod DDoS angreb. En firewall der forsøger at detektere DDoS angreb i internettets kerne så alle mistænkelige pakker bliver droppet før de når til et offer. I de følgende to underafsnit vil der blive beskrevet en sådan løsning.

4.1 Route based packet filtering

Route based packet filtering er en metode hvorpå man kan filtrere pakker med spoofede adresser, og droppe dem. Route based packet filtering er udvidelse af ingress filtre til hele internettet. Disse filtrer kan så ved hjælp af sender og modtager adresserne, og Border gateway protokollen (BGP), kontrollere om disse pakker er reelle pakker, eller om det er angrebs pakker, der skal droppes. Hvis en pakke er blevet sendt af en anden rute, for eksempel pga et servernedbrud et andet sted på nettet, kan dette filter dog stadig komme til at se den som en angrebs pakke og droppe den. I artiklen nævner de at man ved undersøgelser har fundet ud af at disse filtrer skal placeres på omkring 18 % af alle autonome systemer (AS) rundt om i verden, for at kunne fjerne en stor del af alle spoofede pakker. Lige nu er der mere end 35000 AS'er rundt om i verden, hvilket vil kræve en hel del filtre for at virke. En anden ulempe ved at bruge disse filtre er at BGP beskeder skal indeholde en kilde adresse, og dette vil gøre størrelsen

og processerings tiden af BGP beskederne væsentlig større. Disse ingress filtre vil ikke kunne fange reflekterede pakker, da disse er reelle pakker, med en eksisterende kilde og modtager.

4.2 Distributed attack detection

Distributed attack detection (DAD) skal også etableres i internettets kerne. DAD skal detektere DDoS angreb baseret på netværksanomalier og misbrug observeret af en mængde af distribuerede Detection Systems (DS'er). Anomali detektering består både af bestemmelse af normal trafikmønstre og trafikmønstre der afviger 'meget' fra det normale. Trafikintensivering fra en bestemt type pakker kan være parameter for anomalier. Ved detektering af misbrug prøver man at identificere trafik der matcher et kendt angrebsmønster. Eksempelvis vides det at en angriber der bruger programmet Trinoo kommunikerer med sine masters via TCP port 27665, mens en master zombie kommunikerer med slave zombier via UDP port 27444. DS'erne skal spredes over hele internettet for at overvåge og analysere trafikken der der passerer gennem dem, for på den måde at kunne detektere DDoS angreb. Da hver DS kun kan opnår resultater lokalt, skal de udveksle informationer med hinanden. Der kræves derfor en separat kanal hvori DS'erne kan kommunikere. Der er flere design overvejelser der skal lave med hensyn til DS'erne. Hvor mange skal der være, hvordan skal de placeres og ikke mindst hvordan de indbyrdes kan kommunikere. DS'erne danner et netværk der jo også kan blive udsat for DDoS angreb. I den følgende figur vises en state diagram for en distribueret angreb detektering og DS arkitekturen.

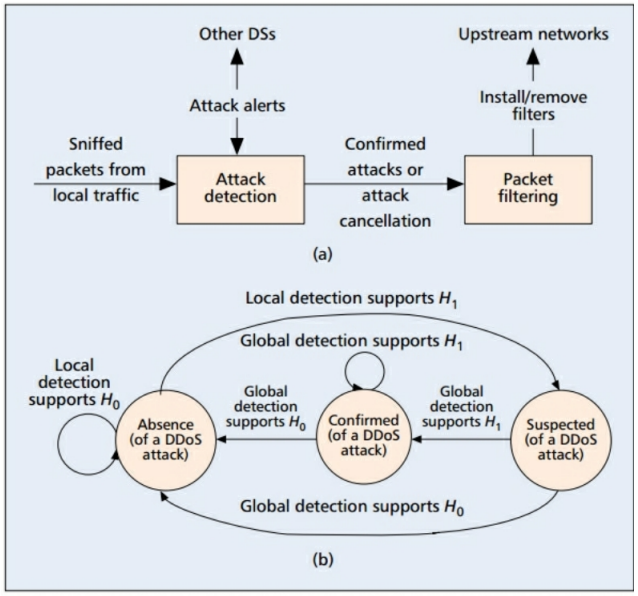


Figure 5. *a) High-level DS architecture and b) a state diagram of two-level attack detection in the distributed detection approach.*

4.3 Problemer og begrænsninger

For at et sådant system skal kunne fungere er der en masse algoritmiske problemstillinger man skal tage højde for. Man skal overveje om man kan ofre noget nøjagtighed til fordel for hastighed, eller omvendt. Samtidig skal systemet også kunne håndtere skiftende brugsmønstre, og kunne håndtere flash-crowds, ved for eksempel store nyheds begivenheder.

5 Konklusion

Vi ved at de eksisterende DDoS angreb kan være meget store og sufistikerede og de forsvarsmekanismer der findes i dag ikke er gode nok, da i det fleste af tilfælderne kan et sufistikeret DDoS angreb lægge et stort virksomhed ned. De eksisterende forsvarsmekanismer skal forbedres markant. En global løsning som beskrevet i rapporten vil formentlig aldrig blive en realitet da det vil kræve for mange ressourcer og mange parter skal involveres. Det er f.eks. ikke sikkert at alle lande vil være med. Det kan dog lavet på et mindre plan.