Försvarsmetoder mot distribuerade överbelastningsattacker

Jonas Laine

Kandidatavhandling i datavetenskap
Handledare: Marina Waldén
Tekniska fakulteten för naturvetenskaper och teknik
Åbo Akademi
2015

Innehåll

1. Inledning

Utvecklingen av nya försvars- och attackmetoder för datorsystem och nätverk skapas hela tiden. Med den moderniserade tiden vi lever i med datorer och IT så är det svårt att hålla sig uppdaterad över alla utvecklingar som händer.

På grund av den snabba utvecklingen från både försvars- och attackmetoder är det svårt att hitta flera officiella artiklar eller böcker som skulle hinna ta upp dessa saker. En ny bok som kommer ut med nya försvarsmetoder är nästan irrelevant inom ett år. På grund av detta så kommer denna avhandling att se på tre olika forskningar och jämföra några av de metoder som nämns i dem med varandra.

Denna avhandling kommer se på tre forskningsgrupper och deras resultat över olika försvarsmetoder mot distribuerade överbelastningsattacker (eng. Distributed Denial of Service attacks). Avhandlingen kommer att i stort sätt använda sig av den engelska förkortingen för distribuerade överbelastningsattacker, DDoS. Avhandling kommer att förklara vad en överbelastningsattack är och hur den fungerar samt vilka åtgärder den orsakar för system den används på. Den ser på vilka hjälpmedel som används och hur ett angrepp utförs. Avhandlingen förklarar skillnaderna på de olika typerna av överbelastningsattacker som finns och i vilka kategorier man ofta brukar klassificera attacker med. Till slut jämförs försvarsmetoder från de tre olika forskningsgrupperna med varandra och en slutlig bedömning utförs över vad som anses vara den mest lämpliga metoden och hur framtiden av försvarsmetoder ser ut.

2. Överbelastningsattack

En överbelastingsattack (eng. Denial of Service attack) är som namnet antyder en överbelastning som inträffar på ett system eller nätverk. Enligt World Wide Web (WWW) så definieras en överbelastningsattack som ”ett angrepp som syftar till att göra en dator eller ett nätverk oduglig för att tillhandahålla normala tjänster” [5]. En överbelastningsattack sägs äga rum endast ifall en dator eller ett nätverks resurser är avsiktligt försämrade eller blockerade som resultat av en annan persons ondsinta åtgärder [1]. Dessa attacker behöver inte nödvändigtvis skada datorn direkt eller permanent men de gör att man inte kommer åt datorns resurser. De vanligaste överbelastningsattacker siktar på nätverksbandbredd eller uppkoppling av en dator. Med bandbredds angrepp flödar man nätverket med en hög mängd trafik som leder till utmattning av lediga nätverksresurser vilket i sin del leder till att man inte kan skicka igenom riktiga förfrågan eller paket.
Med uppkopplingsangrepp så flödar man en dator med en hög mängd kopplingsanrop vilket leder till utmattning av alla tillgängliga operativsystems resurser. Detta gör att dator inte längre klarar av att utföra begäran från användaren.

2.1 Distribuerad överbelastingsattack

När ett angrepp endast kommer från enskild värd eller nätverks nod så talar man om en överbelastningsattack (DoS) [4]. När dessa angrepp kommer från flera värdar eller noder så talar man om distribuerade överbelastningsattacker (DDoS) [6]. Både DoS och DDoS attacker utnyttjar sårbarheter i system och nätverk för att orsaka skada [14]. Idén bakom överbelastningsattacker är att överbelasta ett nätverk. Detta är dock svårt att göra med endast en dator då resurserna ensamt inte räcker till. Med distribuerade överbelastningsattacker använder man upp till 100 000 maskiner för att utföra ett angrepp. Slavdatorer, även kallade agenter eller zombien används för att bygga upp ett större attacknätverk som man kallar för Botnät [2]. Dessa slavdatorer har blivigt övertagna med hjälp av skadliga program och utför attacker ofta utan att datorns egna användare känner till det [source]. Med hjälp av stora nätverk av slavdatorer så krävs det inte stora datorresurser för att göra upp en kraftig överbelastningsattack[14].

Ett visuellt sätt att förstå sig på hur enorma distribuerade överbelastningsattacker är på systemet eller nätverket är att föreställa sig ett sjukhus som har resurser för att sköta om maximalt 100 personer. Om man nu föreställer sig att 100 000 personer samtidigt försöker tränga in sig på sjukhuset för att få vård så kan man börja förstå sig på hur stort problemet är. Dock är det ännu värre då endast 0,1 % av alla som söker vård är faktiskt sjuka och behöver vård. Resten har inget fel utan låtsas att de är sjuka och är endast där för att förhindra de allvarligt sjuka från att få vård. Problemet är att kunna avskilja vem som i verkligheten är sjuk och vem som låtsas.
Samma princip gäller för datorsystem och nätverk då de blir utsatta för DDOS attacker. De har stora problem att skilja åt riktiga användare från zombien och botnät.

2.2 Botnät

För att utföra en DDoS attack så krävs det en stor mängd resurser i form av datorer som man kan använda sig av för att utföra en större attack [7]. Dessa nätverk av datorer kallas för botnät. För att en dator skall bli en del av ett botnät så måste man överföra attackkoden som används för att styra botnäten till datorn. Datorer, speciellt sådana med föråldrade operativsystem som saknar brandväggar eller andra skydd har större chans att bli infekterade och bli en del av botnätet.

Tidigare krävdes manuell genomgång för att identifiera och hitta sårbara datorer och maskiner men allt detta kan nuförtiden göras med automatiska skript [14]. Dessa skript är enkla att bygga upp och använda och gör det enkelt för en användare att bygga upp ett botnät. Själva processen att leta fram sårbara maskiner kallas för skanning (eng scanning). Det är sällan som en person själv skapar attack koden utan oftast så används färdiga attackverktygslådor (eng. Attack toolkits) som har hela attacksystemet automatiserat.

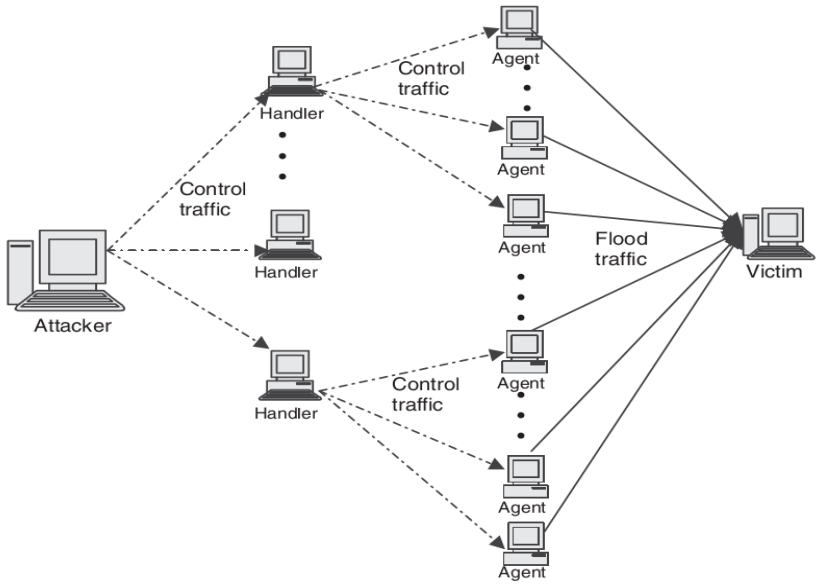
2.3 Agent

En agent är en är en dator som har blivit utsatt för ett skadligt program vilket får den att utföra kommandon som den får av en hanterare [1]. En botnät är uppbyggd av tusentals agenter som används för att utföra DDoS attacken. Ofta talar man också om dessa datorer med andra benämningar som till exempel zombien, slavar eller demoner. Vanligtvis så använder man maskar, trojanska hästar eller bakdörrar av system för att komma åt datorerna och göra dem till agenter [3].

3. DDoS strategi

3.1 Strategi baserad på hanterare

En DDoS attack som använder sig av hanterare är uppbyggd av fyra delar (Figur 1) [1]. Bakom hela attacken ligger själva användaren som utför angreppet. Detta är personen som är själva hjärnan bakom angreppen och som bygger upp hela attacknätverket. För att skydda sig själv och ens identitet bättre används hanterare även kallade mästare (eng. Handler/Master) för att styra attacknätverket och skicka kommandon till agenter. Dessa hanterare är datorer eller andra värdar som tagits över av skadliga program vilket gör att användaren kan kontrollera dem. Dessa hanterare används för att kontrollera de massiva antalet agenter/zombien som utför själva attacken. Det är dessa agenter som skapar DDOS attackerna och orsakar själva skadan och överbelastningen av nätverket eller systmet. Datorer som saknar virusprogram eller brandväggar är ofta datorer som blir utsatta för övertag och blir agenter. Speciellt gamla datorer har en större risk för att bli utsatta för detta [14]. För att undvika snabbare respons från offret eller enklare spårbarhet tillbaka till själva användaren så brukar man ofta använda sig av agenter som finns utanför både användarens och offrets nätverk.

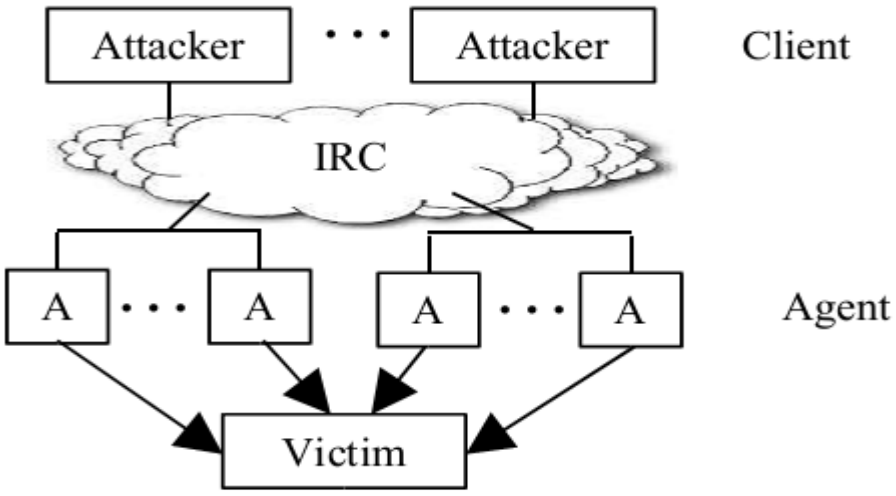


Figur 1: Attacknätverksuppbyggnad med hanterare och agenter. [1]

Själva attacken utförs i fyra faser[1]. Först väljer personen bakom attacken, alltså användaren vilka agenter som skall användas i attacken. Tidigare så måste användarna manuellt gå igenom vilka agenter som kunde användas men dessa funktioner är nuförtiden automatiska. Efter att agentera har valts så placeras attack kod i dessa maskiner som får dem att utföra själva angreppet. De vanliga ägarna av dessa agentmaskiner har ingen aning själv att deras datorer används för att utföra dessa attacker. Efter detta så kommunicerar användaren med hanterarna och ser till att alla agenter som kommer att användas är redo. När allt detta är i ordning så utförs själva attacken. Användaren kan bestämma hur länge själva attacken skall utföras och ifall någon speciell åtgärd skall användas i något fall. Ifall en agents kommunikation följs upp så skulle det leda till en hanterare i stället för den verkliga användaren som ligger bakom attacken.

3.2 IRC-baserad strategi

IRC (eng. Internet Relay Chat) är en teknik för online chattrum som personer använder för att kommunicera med varandra [7][8]. I stället för att använda hanterare så använder man IRC kanaler för att koppla ihop agenter (Figur 2). Det finns vissa förmåner med att använda sig av IRC-baserad tekniker [3]. IRC kanaler använder ofta stora mängder av trafik vilket gör att man enklare kan gömma sig bland den normala trafiken. Det är enklare att dela skadlig kod till agenterna. Man behöver inte själv hålla reda på de agenter som man har med IRC



Figur 2: IRC-baserad DDoS attackuppbyggnad. [8]

3.3 Motiv för överbelastningsattacker

Det kan finnas flera olika motiv för en person att börja skicka ut DDoS-attacker. Olika typer av motiv kan klassificeras enligt följande [3][14]:

- Finansiella/ekonomiska skäl. Idén bakom dessa attacker är att utsätta websidor av företag för DDoS-attacker och på så sätt rejält förhindra användningen av företagets websidor eller till och med ta ner dem helt. Ifall företagen inte vill att de skall utsättas för liknande attacker så måste de betala mutor till gärningsmannen eller sätta ännu större resurser och pengar på att uppgradera deras system så att de inte blir utsatta för liknande attacker i framtiden. Ofta är dessa typer av attacker de farligaste och svåraste att stoppa.
- Revansch. Personer som vill hämnas på någon som de hatar eller ett företag som de känner att har behandlat dem dåligt. Dessa attacker är ofta av lägre kvalitet.
- Ideologisk tro. Personer som tillhör denna kategori har en ideologisk tro för att anfalla deras mål. Dessa kan också vara politiska skäl för att sabotera någon.
- Intellektuell utmaning. Personer i denna kategori använder sig av olika typer av överbelastnings-attacker för att lära sig hur de fungerar och hur bra de försvaras emot. Ofta handlar det om unga personer som vill visa sin skicklighet. I dagens läge så finns det enkla verktyg att använda och hyra ut botnät för att utföra DDoS-attacker vilket underlättar att anfallen lyckas.
- Cyberkrig. Personer i denna kategori hör oftast till militären eller klassificeras som terrorister. Målet för dessa personer är att anfalla kritiska punkter för ett land som t.ex. banker eller vatten/energi infrastrukturer samt telekommunikationer. Personer som utför dessa attacker är vältränade och har stora resurser för sitt tillförfogande.

3.4 Historiska DDoS attacker

Med utveckling av datorer, internet och allting relaterat till dessa så har verktygen för att utföra DDoS attacker också ökat. Med snabbare och kraftigare datorer och bättre och effektivare algoritmer och system för att kontrollera andra datorer så blir det allt enklare att utföra mer kraftfulla DDoS attacker.

Det är svårt att försöka exakt fastslå när de första DDoS attackerna började utföras men man kan uppskatta att det var i slutet av 90-talet [16, 17]. Antalet attacker och storleken på dessa har ökat kraftigt under de senaste åren.

För att sätta utvecklingen i bättre perspektiv så kan man se på skillnaden från 2014 och 10 år tidigare. 2004 så var den största DDoS attacken i storleksklass 8GB/s [15]. Ett årtionde senare så har siffran stigit till 400 GB/s. På endast 10 år så har DDoS attackernas kraftighet stigit 50 gånger.

Ett av de mest kända DDoS attackerna inträffade 18 mars 2013 på Spamhaus webbsidor [12, 13]. Attacken började med en storlek på 90GB/s. Detta räckte dock inte för att ta ner webservrarna men den 22 mars så gjordes det än större attack på 300 GB/s som fick webbsidan att krascha. Detta var under tiden den största utförda DDoS attacken.

I början av 2014 så hade attack-kapaciteten ökat med 33% då CouldFlare uppgav att deras kunder blivigt utsatta för en 400 GB/s attack [11]. Den största utförda DDoS attacken som har upptäckts inträffade i Hong Kong, China i slutet på 2014 under demonstrationer [10]. En attack av storleken 500GB/s uppgavs ha gjorts över ett par nyhetssidor, Apple Daily och PopVote.

Med den takt som dessa attacker verkar öka i storlek så kommer till och med de största webservrarna och nätverken att vara i fara.

4. Typer av DDoS attacker

Man kan klassificera DDoS attacker på två sätt, som banbreddsförbrukande- eller som resursförbrukande attacker [2]. Resursförbrukande attacker använder sig av tekniker som skickar paket som misshandlar nätverkets protokoll kommunikationer eller genom att skicka missbildade paket [8]. Dessa tar upp alla nätverksresurser så att ingen riktig användare kommer åt dem. Bandbreddsförbrukande attacker överbelastar nätverket på olika sätt och delas in i två grupper: flödesattacker och amplifikationsattacker [2].

Utöver dessa huvudtyper så finns det flera tekniker som används för att lura ett försvarssystem för att få den att tro att de paket man skickar är riktiga och för att komma igenom en brandvägg som försöker plocka bort fel sorts trafik.

IP spoofing är en metod som får attackpaketen att se ut att komma ifrån flera olika berättiga klienter [14]. Denna metod används ofta för att förbipassera försvarsmetoder som endast tillåter trafik från berättigade klienter. IP spoofing kan användas för att gömma agentdatorernas position eller för att utföra reflektionsattacker.

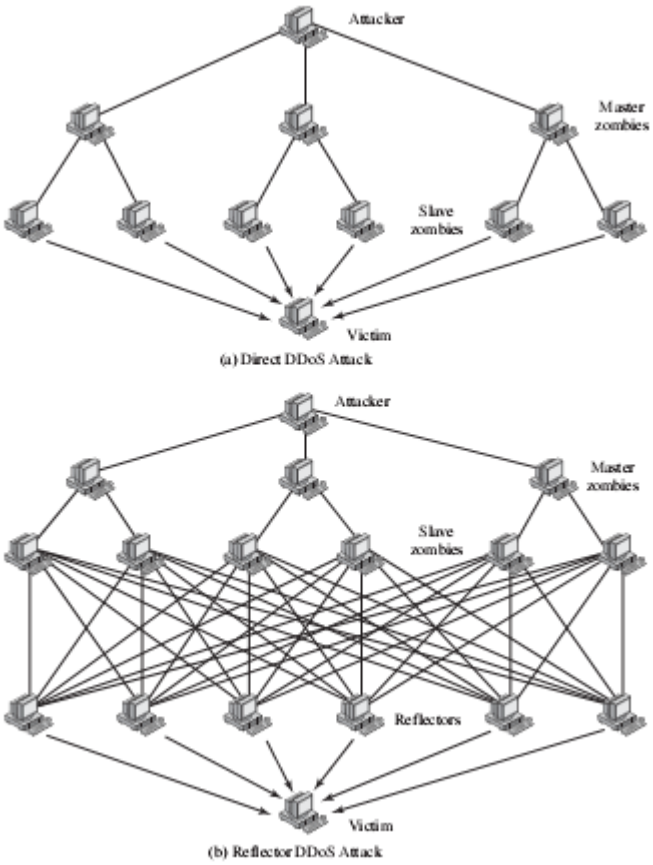
4.1 Bandbredsförbrukande tekniker

4.1.1 Flödesattacker

Flödesattacker är det vanligaste och mest använda sättet att utföra ett DDoS angrepp [14]. Flödesattacker använder sig av stora mängder agent datorer, upp till 100 000 tals, för att överbelasta offrets nätverk med IP trafik. Offrets system saktas ner eller kraschar då nätverksbandbredden blir förstockad [7]. Flödesattacker kan använda sig av både ICMP (eng. Internet Control Message Protocol) och UDP (eng. User Datagram Protocol) paket i attackerna.

Ett sätt att skilja på flödesbaserade DDoS attacker är mellan en direkt attack och en reflektions attack (Figur 3) [4, 9]. Direkta DDoS attacker skickar stora mängder attack paket direkt mot offret via agenter. En av de vanligaste sorters direkta attacker är TCP syn flooding [9]. Med TCP syn flooding så skickar men flera TCP syn paket till offrets nätverk. Nätverket svarar på dessa paket med att skicka en ack (eng. acknowledgement) bekräftelse tillbaka. Attackeraren svarar inte på dessa bekräftelser vilket får offrets nätverk att vänta på ett svar som inte kommer. Detta fyller upp alla förbindelser som offret har vilket gör att verkliga förfrågningar inte mera kan mottas.

Reflektionsattacker är indirekta attacker som använder sig av närliggande noder i nätverket, även kallade reflektorer för att utföra en attack [9]. Attackeraren skickar paket till reflektorer vilket kräver svar från dem. Dessa svar skickas vidare mot offrets nätverk vilket överbelastar nätverket med en massa trafik. Reflektorer behöver inte vara infekterade agent datorer utan man kan skicka paket till vanliga datorer [4].



Figur 3: Visuell bild över direkta och reflektionsattacker. [4]

4.1.2 Amplifikationsattacker

En amplifikationsattack använder agenter för att skicka meddelanden som skickas till alla system i ett subnät [8]. När routerna får emot paketen så kopierar de meddelanden och skickar de vidare till offrets system. En DDoS smurf attack är ett exempel på en amplifikationsattack.

4.2 Resursförbrukande attacker

4.2.1 Protokoll utnyttjande attacker

Protokoll utnyttjande attacker missbrukar olika sorts protokoll för att skapa situationer som systemet inte kan behandla [2]. Ett exempel på en sådan attack är då man missbrukar TCP SYN (eng. Transfer Control Protocol Synchroniser) protokollet och de URG (eng. urgent pointer) fält som finns i paketen som kräver att dessa skall behandlas angelägetsvis. Genom att flöda ett system med en massa TCP URG meddelandet så klarar systemet inte av att behandla dem alla.

4.2.2 Missbildade paket attacker

Attacker som använder sig av missbildade paket använder sig av agenter för att skicka felformade IP paket till offret och få deras system att krascha. IP adress attacker använder samma destinations och ursprungs IP adresser för att förvirra systemet och få den att krascha. Det finns också attacker som använder missbildade paket med garanterade tjänstekvalitets (eng. quality of service) bitar som alla blivit utsatta till 1:or för att kräver mer processtid av systemet för att analyseras

5. Försvarsmetoder

Orsaken varför det är så svårt att skydda sig från DDoS attacker är på grund av brandväggar och andra försvarssystem tolkar DDoS attacker som normal trafik [14]. På grund av att DDoS attacker använder enorma agent-nätverk med flera datorer så kan man inte stänga ut endast en förbindelse och tro att attacken skulle stoppas. Man kan dela in försvarsmetoder i tre olika faser: Förebyggande försvar, upptäckande och filtrering, tillbakaspårande och identifikation[4].

Förebyggande försvar försöker stoppa attacken innan den ens kommer igång genom att identifiera och försöka filtrera bort felaktiga paket. Man kan också använda sig av reserv resurser som tas i bruk ifall en attack skulle börja och som förstärker nätet så att den inte genast skulle gå ner under en attack. En viktig del av förebyggande försvar är att se till att alla datorer och system i nätverket är uppdaterade och har de nyaste säkerhetsuppdateringar installerade [1].

Ifall man blir utsatt för en DDoS attack så är det viktigt att kunna upptäcka och filtrera bort felaktig trafik från systemet eller nätverket [4]. Desto snabbare man kan upptäcka att en attack är på gång desto snabbare kan man reagera på den och utföra åtgärder för att stoppa eller minska på attacken.

Redan under en attack så försöker man hitta den ursprungliga källan bakom attackerna. Ifall man kan identifiera vem som ligger bakom attackerna så kan man enklare stoppa dem och förhindra flera attacker i framtiden från samma ställe. Problemet är dock då användningen av botnät ofta förhindrar att hitta den verkliga personen bakom attackerna.

För att få en bättre uppfattning över hurdana försvarssystem som finns tillgängliga så har 3 forskningsgruppers resultat och ett par av deras försvarsmetoder jämförts.

5.1 Förslag 1

I artikeln Evoluation of Mitigation Metods for Distributed Denial of Service Attack av Rejimol Robinson och Ciza Thomas nämns fyra förslag av försvarsmetoder mot DDoS attacker [2]. Dessa metoder är: Mitigation Model for DDoS Attack with Swarm Network, Mitigation of TCP SYN Flooding with IP Spoofing, Mitigation by Adapitve History-Based Filtering och Probabilistic approach and HCF method. Av dessa så är de två först nämnda metoder mer relevanta i denna avhandling och kommer att ses på någrannare.

5.1.1 Swarmnätverk

Ett svärmnätverk fungerar som ett extra nätverk ovanpå den normala och används för att ge extra tillgänglighet till nätverket under en DDoS attack. Svärmnätverket har möjligheten att omorganisera sig själv under svåra omständigheter som under ett angrepp. Den använder sig av svärm intelligens för att omorganisera sig och kunna köra stora parallella sökningar av lösningar över de problem som ställs på nätverket. Själva nätverket används för att kunna skicka meddelanden mellan klient och server. Nätverket använder sig av flera noder som kommunicerar och koordinerar med varandra.

Svärmnätverk använder sig av Intelligent Water Drop algoritmen. Algoritmen söker fram den snabbaste och mest effektiva vägen i nätverket. Ett svärmnätverk upptäcker inte själv skadlig trafik men den upprätthåller ett effektivt nätverks- och transport system som ser till att verkliga paket och data kommer rätt fram.

5.1.2 TRAP

Den andra försvarsmetoden som tas upp är ett skydd mot TCP SYN flödesattacker som använder IP spoofing. Dessa attacker utnyttjar TCPs trevägs handskakningar för att överbelasta nätverket. För att skydda sig från dessa attacker så används en metod kallad TRAP (eng. TCP probing for Reply Argument Packet). Denna metod är en lindringsmetod (eng. mitigation) på servern som hittar förfalskade IP och lindrar

DDoS attacker. TRAP använder sig av en TCP bekräftelse om kräver en återutsändning från de paket nätverket tar emot. Ifall sändaren inte klarar av att göra detta så anser servern att paketet är förfalskad. Metoden använder sig av fyra moduler för att kunna uppfylla sin uppgift: Protokoll analyserande modul, detektor, lärande/inspelande paket analys och TCP avkännare.

5.2 Förslag 2

Artikeln ”A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks” av Saman Tagahavi Zaargar, James Joshi och David Tipper nämner flera förslag av försvarsmetoder mot flödesbaserade DDoS attacker[3]. Artikeln delar in försvarsmetoderna enligt den protokollnivå som attackerna baserar sig på, nätverk/transport- eller applikationsnivån. De försvarsmetoder som kommer att nämnas är av nätverk/transport nivån då dessa är mer använda tekniker.

5.2.1 D-WARD

D-WARD är en försvarsmetod som strävar till att upptäcka flödesattack liknande trafik genom att övervaka både in- och utgående trafik ur sitt nätverk. Den trafik som övervakas jämnförs med normalt flöde vilket är fördefinierad inom vissa gränser. Ifall metoden upptäcker onormala flöden så filtreras de bort. D-WARD är en källbaserad försvarsmekanism vilket betyder att den försöker upptäcka flödesattacker från attackerarens nätverk då de skickas iväg från agenter. Detta betyder att metoder egentligen endast skyddar andra nätverk men inte sitt eget ifall de andra nätverken inte använder D-WARD. Ifall att attackerna utförs med normala flöden så kommer D-WARD inte att upptäcka dem.

5.2.2 Hybrid

Problemet med flera DDoS försvarsmetoder är att de baserar sig ofta på en viss typ av försvar och saknar samarbete mellan olika typers försvarsmetoder. Hybrid metoder använder flera typers försvar på olika ställen i ett nätverk för att sammanbinda flera sorts försvarsmetoder till ett större och mer omfattande paket.

Kompetensbaserad mekanism (eng. Capability-based mekanism) är en hybrid modell som endast tillåter trafik som den har bekräftat. Sändaren måste be om en kortsiktig bekräftelse från mottagaren för den kan skicka sitt meddelande. Efter att sändaren blivit godkänd så markeras paketen med en stämpel som routers godkänner och låter kommer igenom till nätverket. Bekräftade paket får förkörsrätt vid de routers som finns i nätverket medan obekräftade paket ignoreras. Nätverket använder flera verifikationspunkter runt nätverket för att uppehålla att endast godkända paket tas emot.

5.3 Förslag 3

Boken ”Internet Denial of Service: Attack and Defense Mechanisms” av Jelena Mirkovic Sven Dietrich, David Dittrich och Peter Reiher förklarar i bra detalj vad en överbelastnings attack är, dess funktioner, användningssätt samt olika försvarsmetoder och sätt som man kan använda sig av för att skydda sig mot en överbelastningsattack [14].

5.3.1 Pushback

Pushback är en metod som ursprungligen uppfanns av en forskningsgrupp i CERT. Iden bakom Pushback metoder är att helt enkelt att koppla bort vissa kopplingar vid routern för att se ifall det kan minska på attacken. Pushback används tillsammans med en annan teknik, lokal ACC (eng. Aggregate Congestion Control) för att

upptäcka överbelastning på router och avlägsna dem. Efter att en stockning har upptäckts så används ACC för att skapa ett filter som begränsar överbelastningsattacken. Pushback används sedan för att propagera denna filter till närliggande noder i nätverket för att minska på angreppet. Denna typs försvarsmetod fungerar bäst mot flödesattacker.

5.3.2 DefCOM

DefCOM är ett distribuerat system som kopplar samman källbaserade, offerbaserade och kärnbaserade nätverksförsvar. Systemet kan känna igen en pågående attacker och minska på attacktrafiken medan verklig trafik fortfarande kan överföras. Den är uppbyggd av tre typer av noder vilka ofta är routers. Alertgeneratorer upptäcker attacken, hastighetsbegränsare upprätthåller enkla begräsningar över all trafik som går mot offret och klassificerare som kan separera äkta paket från oäkta och sedan markera de äkta med en klassifikation.

När en attack inträffar så spårar DefCOM all trafik som skickas till offret (både äkta och förfalskade paket) och börjar gå igenom trafiken. Klassificerare börjar sedan gå igenom trafiken börjandes från källor som ligger närmast offret. Alla paket blir markerade som äkta, misstäktsamma eller omarkerade. Med detta så skapas det ett 3-nivås service som först kommer att ge tillgång till nätverket för äkta paket.

5.4 Jämförelse av försvarsmetoder

Det är svårt att kunna jämföra och veta vilken försvarsmetod som skulle fungera då man inte själv kan pröva ut dem och se hur de reagerar och hanterar en DDoS attack. De olika försvarsmetoderna används också för att stoppa olika typers DDoS attacker. De är också uppbyggda för olika system vilket gör avgörandet mellan vilken försvarsmetod som är bäst svårt. Dock kan man kolla på de olika metodernas för- och nackdelar för att få en bättre uppfattning över vilka eventuella brister de har och vilka som teoretiskt sätt skulle fungera bäst. Tabellen nedan listar de största styrkorna och svagheterna för de försvarssystem som nämnts.

Tabell 1: För- och nackdelar för försvarssystem [2][3][14]

Metod	Fördelar	Nackdelar
Svarmnätverk	Robust transport nätverk som uppehåller kommunikationen.	Kräver extra bandbredd p.g.a. kommunikation mellan noder i svärmen.
TRAP	Eliminerar TCP SYN flödesattack som använder IP spoofing.	Endast effektiv metod för en specifik typ av attacker.
D-WARD	Filtrerar bort flödesattacker redan vid källan av attacken före den når sitt mål.	Skyddar inte sitt eget nätverk utan måste lita på andra metoder för detta.
Hybrid	Uppbyggd av flera försvarsnoder på flera ställen i nätverken.	Kräver samarbete mellan flera nätverksleverantörer för att byggas upp.
Pushback	Effektivt försvars mot flödesbaserade attacker.	Kräver mera prestation från routers. Routers måste också känna till metoden för att fungera korrekt.
DefCOM	Klarar av att filtrera bort attackpaket och låta riktiga paket komma fram.	Endast i en tidig design och implementations fas.

6. Diskussion

En del av problemet med både utvecklingen och användningen av olika DDoS försvarsmetoder är samarbetet mellan individer och enheter. Det finns flera företag och personer som ettdera forskar eller utvecklar nya tekniker för att skydda sig mot olika nätattacker inklusive överbelastningsattacker. Dock verkar det finnas en väldigt liten del som sammarbetar för att hitta en gemensam lösning för problemet. I stället utvecklar alla sin egen lösning som kanske skulle kunna förstärkas ifall man jobbade tillsammans. Ifall att företag lyckas utveckla en ny försvarsmetod så vill de inte dela med sig denna metod till någon annan, speciellt inte gratis. Detta är förståeligt men betyder att andra mindre företag och individer lider då de inte får tillgång till lika bra skydd.

Det finns flera problem med att försöka dela med sig informationen och tillverka ett ordentligt försvar. Ett problem är att personerna som utför attackerna mer sannolikt får tag på informationen av försvarsmetoderna. Med detta så kan de ändra på sina strategier och anfallsmetoder för att igen undvika eller lura de försvarsmetoder som används. Det är också svårt att kunna pröva på egna försvarssystem man skapar för att det skulle krävas en enorm mängd med datorer för att skapa lika stora attacker som försvarsmetoderna skall klara av att skydda sig ifrån.

Enligt min åsikt så krävs det större samarbete mellan olika forskningsgrupper och större nätleverantörer som producerar försvarsmetoder för att kunna bygga upp ett bättre försvar mot DDoS attacker. Hybrid försvarsmetoder verkar vara en bra lösning som ett mer globalt försvar. Dessa metoder kommer dock att kräva samarbete mellan personer och enheter vilket alltid kan vara svårt att uppfylla.

7. Sammanfattning

En överbelastningsattack (DoS) är ett angrepp som utförs på ett datorsystem eller ett nätverk för att förhindra eller totalt stoppa systemet eller nätverken. Överbelastningsattacker som utförs från flera datorer kallas för distribuerade överbelastningsattacker (DDoS). DDoS attacker använder enorma botnät som är uppbyggda av flera hanterare som kontrollerar tusentals agent. Agenter är datorer som tagits över med skräpprogram eller liknande och används utan att själva veta om det. Med hjälp av botnät så kan attackerare använda

Det finns tre nivåer av DDoS försvar. Förebyggande försvar försöker undvika att bli överfallna och fungerar som ett skydd före en attack inträffas. Filtreringsförsvar försöker filtrera bort felaktiga paket och användare under en attack. Identifiering och tillbakaspårning används för att kapa av attacken vid källan och se till att man inte i framtiden blir utsatt från samma ställe.

Varje DDoS försvarsmetod har sina för- och nackdelar. De flesta försvarssystem fokuserar endast på att hindra en viss sort attack vilket gör dem sårbara för andra sorts attacker. Hybrida försvarsmetoder är en nyare sorts försvar som sammanbinder olika försvarsmetoder i ett för att skapa ett mer utvidgat försvar.

En sak som är viktigt att inse att fastän nya försvarsmetoder konstant utvecklas så utvecklas också nya attackstrategier och metoder. Attacker blir allt mer större då kraftigare datorer utvecklas och det är viktigt att försvarsmetoder hänger med i utvecklingen. För att skapa ett bättre skydd mot DDoS attacker så krävs det ett större samarbete mellan utvecklare och internetleverantörer som förser skydd mot dessa attacker.

Referenser

[1] Aikaterini Mitrokotsa and Christos Douligeris (2007), Denial-of-Service Attacks in: Network Security: Current Status and Future Directions

[2] Rejimol Robinson R. R. and Ciza Thomas (2011), Evaluation of Mitigation Methods for Distributed Denial of Service Attacks

[3] Saman Taghavi Zargar, James Joshi, David Tipper (2013), A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks

[4] William Stallings (2011), Distributed Denial of Service Attacks in: Network Security Essentials: Applications and Standards 4th edition

[5] Lincoln Stein, John Stewart (2014) Securing against Denial of Service attacks, http://www.w3.org/Security/Faq/wwwsf6.html

[6] Tao Peng, Christopher Leckie and Kotagiri Ramamohanarao (2007) Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems

[7] Esraa Alomari and Selvakumar Manickam (2012) Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art

[8] Spephen M. Specht and Ruby B. Lee (2004) Distributed Denial of Service: Taxanomies of Attacks, Tools and Countermeasures

[9] Rocky K. C. Chang (2002) Defending against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial

[10] Parmy Olson (2014) The Largest Cyber Attack In History Has Been Hitting Hong Kong Sites, http://www.forbes.com/sites/parmyolson/2014/11/20/the-largest-cyber-attack-in-history-has-been-hitting-hong-kong-sites/

[11] Steven Musil (2014) Record-breaking DDoS attack in Europe hits 400Gbps, http://www.cnet.com/news/record-breaking-ddos-attack-in-europe-hits-400gbps/

[12] Ian Thomson (2013) London schoolboy cuffed for BIGGEST DDOS ATTACK IN HISTORY, http://www.theregister.co.uk/2013/09/27/london_schoolboy_arrested_for_biggest_ddos_attack_in_history/

[13] Matthew Prince (2013) The DDos That Almost Broke the Internet, https://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet/

[14] Jelena Mirkovic, Sven Dietrich, David Dittrich, Peter Reiher (2005) Internet Denial of Service: Attack and Defense Mechanisms

[15] Arbor Networks (2014) Worldwide Infrastructure Security Report

[16] Stefanie Hoffman (2013) DDoS: A Brief History, https://blog.fortinet.com/post/ddos-a-brief-history

[17] Joseph Cox (2014) The History of DDoS Attacks as a Tool of Prostest, http://motherboard.vice.com/read/history-of-the-ddos-attack