HÖGSKOLAN SKÖVDE

Institutionen för kommunikation och information
Examensarbete i datavetenskap 10p
C-nivå
Vårterminen 2006

Distribuerade belastningsattacker
Klassificering och utvärdering

Erik Brolin

Distribuerade belastningsattacker

Examensrapport inlämnad av Erik Brolin till Högskolan i Skövde, för Kandidatexamen (B.Sc.) vid Institutionen för kommunikation och information. Arbetet har handletts av Jesper Holgersson.

2006-10-13

Härmed intygas att allt material i denna rapport, vilket inte är mitt eget, har blivit tydligt identifierat och att inget material är inkluderat som tidigare använts för erhållande av annan examen.

Signerat: _____

Distribuerade belastningsattacker

Erik Brolin

Sammanfattning

Användandet av Internet ökar varje år och företag blir i takt med detta mer och mer beroende av att kunna erbjuda sina kunder tjänster här. Ett hot mot dessa tjänster är den distribuerade belastningsattacken. En belastningsattacks mål är att göra en server på Internet otillgänglig för vanliga användare genom att antingen överbelasta den med stora mängder data för att skada serverns bandbredd eller att göra ett stort antal uppkopplingsförfrågningar för att skada serverns kapacitet att behandla meddelanden. Vid en distribuerad belastningsattack använder en angripare sig av många datorer på Internet vilka inte är dennes egna för att göra sin attack mycket starkare. Målet med detta projekt har varit att klassificera och utvärdera skyddsmetoder mot detta med avseende på faktorerna kostnad samt effektivitet. Resultatet visar att den mest kostnadseffektiva skyddsmetoden är klassbaserad köbildning.

Nyckelord: Distribuerade belastningsattacker, DDoS, informationssäkerhet, nätverkssäkerhet, skyddsmetoder.

Innehållsförteckning

1 Introduktion

Bara mellan år 2000 och 2006 har användandet av Internet i världen ökat med över 200 % (Miniwatts Marketing Group, 2006). Företag använder också Internet i allt större utsträckning för att erbjuda sina kunder tjänster där. Många av dessa företag är beroende av dessa tjänster och skulle tjänsterna göras otillgängliga kan det innebära ekonomiska förluster för företagen eller ge dem ett dåligt rykte.

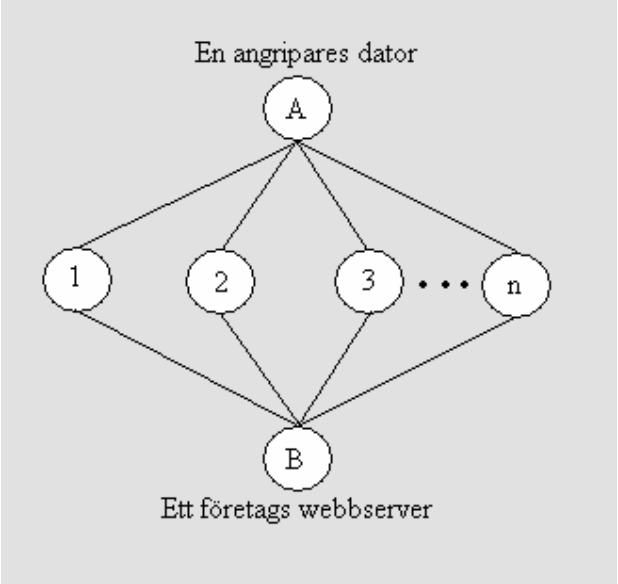
Syftet med informationssäkerhet är att förebygga hot mot svagheter hos system. Ett exempel på ett sådant hot är hot mot tillgängligheten. Ett företags webbserver behöver finnas tillgänglig då den kan vara av stor vikt för företaget. En form av angrepp mot tillgängligheten är avbrottsattacker vars syfte är att hindra att paket som skickas till servern inte kommer fram eller inte behandlas (Pfleeger, 2003). En form av avbrottsattacker är belastningsattacker, vilka enligt Douligeris och Mitrokotsa (2004) gör en server på Internet otillgänglig för vanliga användare genom att antingen överbelasta den med stora mängder data för att skada serverns bandbredd eller att göra ett stort antal uppkopplingsförfrågningar för att skada serverns kapacitet att behandla meddelanden. En distribuerad belastningsattack är en belastningsattack i vilken angriparen tar hjälp av ett stort antal datorer på Internet, vars ägare är ovetande, som alla samarbetar med att attackera servern samtidigt. Detta gör attacken mycket kraftfull och svår att skydda en server mot.

Problemet som denna rapport behandlar är att utföra en klassificering av skyddsmetoder för distribuerade belastningsattacker. Dessa skall sedan utvärderas med avseende på två faktorer. Dessa faktorer är kostnaden för att implementera metoden samt dess effektivitet.

Resultatet som presenteras i kapitel 5 visar en vanlig klassificering som gjorts av bland andra Douligeris och Mitrokotsa (2004), Mirkovic och Reiher (2002) samt Lee och Specht (2003). En klassificering anpassad till problemet presenteras och de metoder som klassificerats utvärderas och jämförs baserat på deras kostnadseffektivitet.

2 Bakgrund

Följande kapitel inleds med ett vanligt förekommande problemscenario i nätverk. Enligt Douligeris och Mitrokotsa (2004) är scenarios likt det som beskrivs nedan ett av de största hoten bland säkerhetsproblemen hos Internet idag.



Figur 1 - Exempel på en attack

Figur 1 visar system A – en angripares dator, system B – ett företags webbserver, samt ett godtyckligt antal system däremellan, alla uppkopplade mot Internet. Angriparen tar hjälp av system 1 till n genom att installera attackkod på dessa system. Systemen används för att utföra en kraftfull, gemensam attack mot företagets webbserver. Ägarna till de godtyckliga systemen förblir under förloppet ovetande om angreppet. Efter ett lyckat angrepp är webbservern inte längre kapabel att svara på meddelanden från andra system.

2.1 Informationssäkerhet

Ovanstående scenario är ett hot mot det som kallas informationssäkerhet. Syftet med informationssäkerhet är att utveckla sätt att förebygga att svagheter hos datasystem utnyttjas. För att ett system ska klassas som säkert skall det uppfylla ett antal huvudmål som finns inom informationssäkerhet. Enligt Pfleeger (2003) finns tre huvudmål inom informationssäkerhet. Dessa mål är sekretess (eng. confidentiality), integritet (eng. integrity) samt tillgänglighet (eng. availability). Ofta används även spårbarhet (eng. traceability) som ett viktigt mål.

2.1.1 Sekretess

Information skall enbart kunna tas del av av personer med rätt behörighet. Om till exempel ett e-postmeddelande skulle kunna läsas av andra personer än den tänkta mottagaren är det ett hot mot sekretessen.

2.1.2 Integritet

Det är även ett mål att informationen som mottagaren får är riktig och oförändrad. Om informationen blivit modifierad på vägen till mottagaren, det vill säga att någon har förändrat, lagt till eller tagit bort information, är det ett hot mot integriteten.

2.1.3 Tillgänglighet

Att information är tillgänglig innebär helt enkelt att mottagaren skall kunna tillgodogöra sig informationen. Får mottagaren inte tillgång till den i rätt utsträckning eller inom rimlig tid är detta ett hot mot tillgängligheten. Det inledande scenariot är ett exempel på en attack mot tillgängligheten.

2.1.4 Spårbarhet

Spårbarhet innebär att det skall vara möjligt att spåra varifrån information kommer. Det skall även vara möjligt att spåra de förändringar av informationen som skett, samt vem som har utfört dessa. Vid en attack som den i det inledande scenariot är det viktigt att kunna spåra vilka system det är som utfört angreppet för att enklare kunna förhindra en upprepad attack.

2.2 Databrott

I detta kapitel presenteras en bakgrund till databrott för att visa vilka som kan tänkas utgöra en hotbild mot informationssäkerhet och anledningar som finns till att utföra ett brott av detta slag.

Vad som definieras som ett databrott kan vara svårt att avgöra. Enligt Pfleeger (2003) är detta på grund av att vissa lagstiftare har svårt att förstå datavärlden, vilket kan bero på att området utvecklas snabbt. Att ändra eller skapa nya lagar tar lång tid vilket inte matchar den snabba utvecklingen. Något som ytterligare försvårar definitionen är att en dator kan ha många roller vid ett brott. Den kan vara målet för brottet eller verktyget som används för att utföra det.

2.2.1 Utövare

Pfleeger (2003) delar in utövare av databrott i tre klasser; karriärsbrottslingar, crackers och amatörer, som alla har olika anledningar till att utföra dessa brott.

- **Karriärsbrottslingar**

  Det finns personer som professionellt sysslar med databrott, det vill säga personer som livnär sig på det. Detta kan vara genom att till exempel utföra en belastningsattack (eng. Denial of Service attack) mot ett företags server för att sedan kräva pengar för att avbryta attacken.

- **Crackers**

  Crackers är användare med högt tekniskt kunnande som medvetet utför databrott så som att bryta in på servrar där de inte har behörighet. Men crackers behöver inte vara karriärsbrottslingar som gör det för att tjäna pengar utan kan ha andra andledningar (se nedan) att medvetet bryta sig in i ett system.

- **Amatörer**

  Det kan även vara amatörer som utför dessa brott. Det behöver inte nödvändigtvis vara så att de ens vet att den handling de utför är ett brott. Ett ofta förekommande databrott bland vanliga användare (det vill säga ej karriärsbrottslingar eller crackers) är brott mot upphovsrätten, vilket vanligtvis tar formen av fildelning över Internet.

2.2.2 Motiv

Det finns många olika anledningar till att databrott begås, så som utmaning, berömmelse, pengar och ideologi. Det är viktigt att se vilka motiv som kan finnas till att begå ett brott för att kunna förutsäga vilka som skulle kunna tänkas attackera till exempel ett företags server, menar Pfleeger (2003).

- **Utmaning**

  En anledning till att begå ett brott är utmaningen. Det finns crackers som bryter sig in i datasystem enbart för att bevisa för andra, eller sig själva, att de kan eller för att visa systemets ägare att deras system är för dåligt skyddat.

- **Berömmelse**

  Sedan finns det de som till exempel bryter sig in system enbart för att bli erkända inom datavärlden för att vara skickliga crackers.

- **Pengar**

  Pengar är även en anledning till att databrott begås. Personer som begår brott av denna anledning kallas karriärsbrottslingar (se ovan).

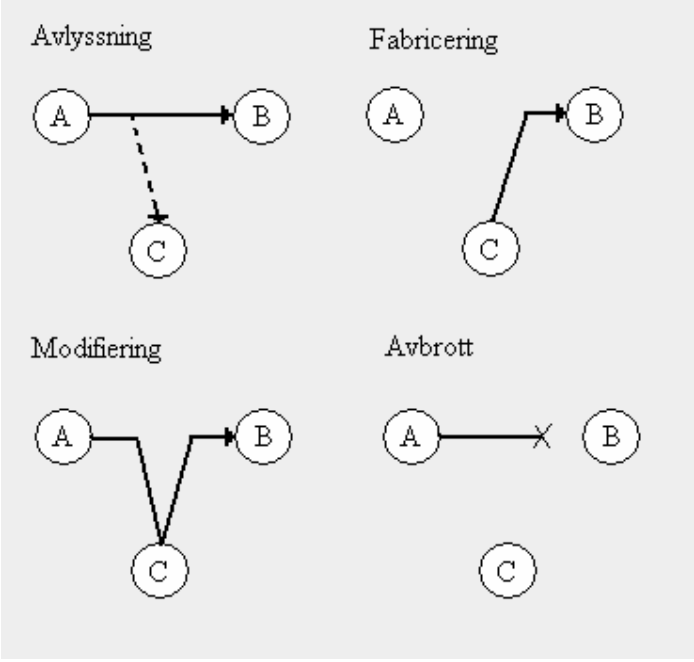
- **Ideologi**

  Det finns de som begår brott på grund av sin ideologiska övertygelse. Ett exempel på detta är när svenska Antipiratbyrån, en ekonomisk förening vilken på order av stora film- och spelbolagsorganisationer bedriver jakt på personer som bryter mot upphovsrätten (Björn Gregfelt, 2005), utsattes för en belastningsattack vilken gjorde deras webbserver oåtkomlig. Enligt Urban Lindstedt (2005) skedde denna attack på grund av att personer kände sig kränkta i och med att Antipiratbyrån samlade in privatpersoners IP-adresser vilket bröt mot personuppgiftslagen.

De system som väljs att bli attackerade varierar också i samband med vilka anledningarna till att utföra en attack är. Det kan vara system med hög säkerhet, låg säkerhet eller helt enkelt vara ett slumpmässigt valt system (Pfleeger, 2003). System med hög säkerhet kan locka crackers att utföra en attack eftersom ju högre säkerheten är, desto större blir utmaningen. Är säkerheten låg kan det locka amatörer att attackera eftersom det är enkelt.

2.3 Attackkategorier

Pfleeger (2003) delar upp de attacker som förekommer i fyra kategorier. Dessa kategorier är avlyssning (eng. interception), modifiering (eng. modification), fabricering (eng. fabrication) samt avbrott (eng. interruption). Figur 2 beskriver fyra scenarios vilka exemplifierar varje kategori. Varje scenario består av två till tre system (A, B och C) samt ett meddelande som skall skickas från system A till system B.



Figur 2 - Attackkategorier

2.3.1 Avlyssning

System A skickar ett meddelande till system B. Men system B, vilket är tänkt att vara den enda mottagaren, är inte ensam om att få meddelandet. Även system C snappar upp det. Trots att meddelandet nådde sin destination är det ett det ett stort hot mot sekretessen om tredje parter kan ta del av information som inte är menad för dem.

2.3.2 Fabricering

I det andra scenariot skickar system C ett meddelande till system B, men sätter avsändaradressen på meddelandet (eng. address spoofing) till system A:s adress istället för sin egen. På det viset kommer system B tro att meddelandet kom från system A. Detta är ett hot mot både integriteten, eftersom informationen inte är riktig eftersom den skapades av fel källa, och spårbarheten eftersom den rätta avsändaren inte går att spåra.

2.3.3 Modifiering

System A skickar i det tredje scenariot ett meddelande till system B, men istället för att gå raka vägen till B, fångas det upp av system C som modifierar meddelandet och sedan skickar det vidare till B. Även detta är hot mot spårbarhet och integritet med samma anledningar som i föregående scenario.

2.3.4 Avbrott

I det fjärde scenariot försöker system A skicka ett meddelande till system B. Meddelandet når dock aldrig mottagaren. Anledningar till detta är till exempel att någon nätverksutrustning mellan de båda systemen inte fungerar som tänkt eller att system B:s möjlighet att ta emot meddelande har satts ur funktion. Interruption är ett hot mot tillgängligheten eftersom system B inte är tillgängligt för att ta emot meddelandet. Angreppet i det inledande scenariot var därmed en sorts avbrottsattack.

2.4 Avbrottsattacker

Avbrottsattacker har som mål att göra ett system otillgängligt eller drastiskt minska den mängd data det kan ta emot eller behandla, så att kopplingarna mellan systemet och andra system som försöker kommunicera med det blir brutna. Det finns ett antal olika sätt att gå tillväga för att göra detta.

2.4.1 Transmission failure

Ett sätt att förhindra att data når ett visst system är, enligt Pfleeger (2003), att göra det fysiskt otillgängligt. Detta kan vara genom att exempelvis klippa av en kabel eller förstöra någon hårdvara mellan de båda systemen vilka försöker kommunicera med varandra.

2.4.2 Traffic redirection

Pfleeger (2003) menar att ett annat sätt att göra ett system otillgängligt är att avleda dess trafik till någon annan plats. Internet är uppbyggt av routrar vilka hjälps åt för att hitta den bästa (kortaste, billigaste och mest tidseffektiva) vägen mellan system. Varje router har en tabell över hur väl den kan nå olika system på Internet, de kan dock bara kommunicera med de routrar de är direkt kopplade till. Om en angripare kan ta kontroll över en router kan denne få den att säga till sina grann-routrar att den har den bästa vägen till alla andra system. Då kommer alla andra routrar vidarebefordra de meddelanden som kommer till dem hit och när meddelandena kommit hit kan routern helt enkelt ta och kasta dem, vilket innebär att de har blivit avledda från målsystemet och inte kommer att nå fram.

2.4.3 DNS-attacker

En attack liknande den i föregående kapitel är DNS-attacken. En DNS (Domain Name Server) är en server som innehåller översättningar mellan domännamn och IP-adresser. Exempelvis kan denna server veta att domännamnet www.google.com har IP-adressen 64.233.183.103. Om en DNS saknar översättning på ett namn skickar den förfrågningar till andra DNSer tills den har adressen. Enligt Pfleeger (2003) kan detta missbrukas på så sätt att om en angripare får kontroll över en DNS kan han/hon lägga in falska översättningar och på så vis avleda trafiken som är tänkt att gå till målsystemet.

2.5 Belastningsattacker

En mer avancerad form av avbrottsattacker är så kallade belastningsattacker (eng. Denial of Service attacks). Scenariot som beskrevs i början av detta kapitel är en form av belastningsattack. Douligeris och Mitrokotsa (2004) beskriver belastningsattacken som en attack vilken syftar till att göra ett nätverk inkapabelt att tillhandahålla dess tjänster genom att påverka antingen nätverkets bandbredd genom att överbelasta det med stora mängder data eller dess möjlighet att behandla meddelanden genom att överbelasta det med ett stort antal uppkopplingsförfrågningar.

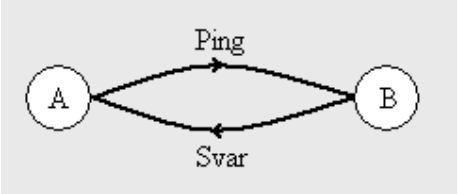
2.5.1 Connection flooding

Att överbelasta en uppkoppling med så mycket data att systemet hindras från att svara på andras meddelanden är den mest primitiva formen av belastningsattacker. Mer avancerade attacker använder sig av Internetprotokoll för att göra attacken effektivare. En sådan protokollgrupp är ICMP (Internet Control Message Protocols) vilken används vid nätverksdiagnostik. ICMP innehåller protokoll som till exempel Ping och Echo. Vid användandet av Ping skickas ett meddelande till ett system som får förfrågan att svara på detta. Detta används till att se om ett system är tillgängligt och fungerande, även till att se hur lång tid det tar för ett meddelande att förflytta sig från det första systemet till det andra, behandlas och sedan förflytta sig tillbaka igen. Följande exempel är ett test av ICMP-protokollet ping.

```
C:\>ping www.google.com

Skickar signaler till www.l.google.com [64.233.183.103] med 32
byte data:

Svar från 64.233.183.103: byte=32 tid=139ms TTL=242
Svar från 64.233.183.103: byte=32 tid=123ms TTL=242
Svar från 64.233.183.103: byte=32 tid=123ms TTL=242
Svar från 64.233.183.103: byte=32 tid=149ms TTL=242

Ping-statistik för 64.233.183.103:
    Paket: Skickade = 4, mottagna = 4, Förlorade = 0 (0 %),
Ungefärligt överföringstid i millisekunder:
    Lägsta = 123 ms, Högsta = 149 ms, Medel = 133 ms
```

Kommandot ping www.google.com skrevs i ett kommandoradsfönster med ovanstående resultat. Det egna systemet försöker skicka fyra paket till systemet med IP-adressen 64.233.183.103 som www.google.com är länkad till. I detta fall mottogs alla paket av målsystemet och tiden det tog för paketet att skickas returneras på skärmen.

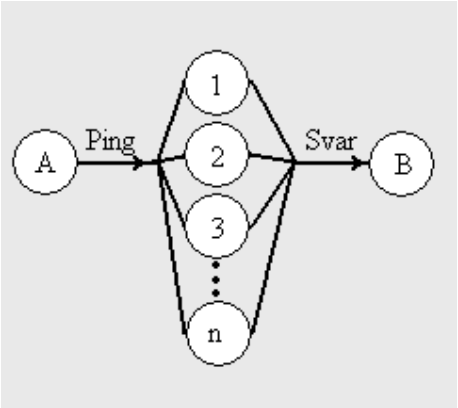
Echo-protokollet skickar en mängd data till en mottagare. Denne mottagare skickar sedan tillbaka samma data oförändrad. Echo används för att kontrollera om ett kommunikationslänken är pålitlig. Båda dessa protokoll kan användas för att utföra en belastningsattack (Pfleeger, 2003). Tre exempel på detta är Ping of Death, Smurf och Echo-Chargen. I dessa exempel är system A angriparen och system B målet.



Figur 3 - Ping of Death

- **Ping of Death**

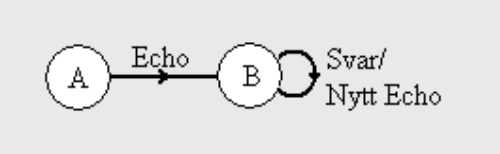
Pfleeger (2003) beskriver den så kallade Ping of Death-attacken (se figur 3) som en av de enklaste attackerna. System A skickar helt enkelt ut så många ping-paket som möjligt för att försöka överbelasta system B genom att ge det mer paket att svara på än det klarar av. Hur lyckad den här attacken kan bli som bäst beror på angriparens egen bandbredd. Om bandbredden hos system A är mindre än bandbredden hos system B kommer angriparen ensam aldrig att klara av att överbelasta målet med en sådan här attack. Om det tvärtom är så att system A har mer bandbredd har attacken en chans att lyckas. Dougligeris och Mitrokotsa (2004) menar att om dessa ping-paket har större storlek är den maximala standardstorleken på IP-paket kan det få effekten att system B kraschar.



Figur 4 - Smurfattack

- **Smurf-attack**

Enligt Pfleeger (2003) är den så kallade Smurf-attacken (se figur 4) en variant av ping-attacken. System A genererar ett ping-paket, men istället för att bara skicka det direkt till system B görs paketet till ett broadcast-meddelande. Meddelandet skickas då till alla system i ett utvalt nätverk. System A sätter även paketets avsändaradress till system Bs, vilket innebär att alla system i nätverket kommer skicka sina svar till B istället för A. Detta innebär att attacken blir kraftfullare när resurserna hos många system används på en gång för att angripa målet.



Figur 5 - Echo Chargen-attack

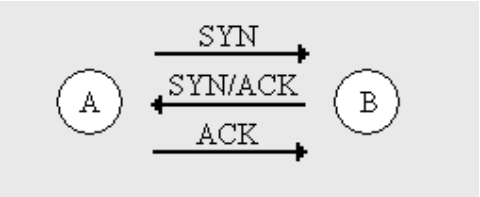
- **Echo-Chargen-attack**

Pfleeger (2003) beskriver Chargen (character generator) som ett protokoll vilket genererar en slumpmässig ström av tecken vilket används till att mäta kapaciteten hos ett nätverk. Detta tillsammans med Echo-protokollet används till den så kallade Echo-Chargen-attacken. System A startar en chargenprocess vilken genererar data i form av echo-paket (se figur 5). Sedan börjar systemet skicka strömmar av dessa paket till system B vilket skickar tillbaka dem till system A. Eftersom datan fortfarande är echo-paket försätts de båda systemen i en loop.

En mer kraftfull variant av detta är när system A sätter avsändaradressen på paketen till B:s adress, eftersom system B då kommer skicka echo-paket till sig själv och försätts på så sätt i en oändlig loop utan att system A påverkas.

2.5.2 SYN flood

Även TCP-protokollet har svagheter som kan utnyttjas av angripare för att utföra en belastningsattack. Detta protokoll är sessionsbaserat och för att inleda en session mellan två system utförs en trevägshandskakningsprocedur (eng. Three-way Handshake). I figur 6 skickar system A ett SYN-meddelande (synchronize) till system B. System B svarar då med ett SYN/ACK-meddelande (synchronize/acknowledge). För att förklara kommunikationslänken öppen och redo att användas skickar system A ett ACK-meddelande till B.



Figur 6 - Handskakningsproceduren

Pfleeger (2003) beskriver att hos system B finns en kö kallad SYN_RECV där paket hamnar för vilka ett SYN/ACK har skickats men inget ACK har mottagits än. Storleken på denna kö är begränsad, vilket gör att en angripare kan skicka många SYN-meddelanden men sedan avstå från att skicka ett ACK. Ett paket i SYN_RECV tas så småningom bort om det inte fått ett ACK, men om system A skickar tillräckligt många SYN på kort tid blir kön full och kan inte ta emot fler SYN-meddelanden från något annat system. System A kan även ändra avsändaradressen för varje SYN det skickar, dels för att dölja sin identitet, dels för att göra varje meddelande unikt vilket gör det svårt för system B att avgöra vilka paket som är från vanliga system.

2.5.3 Klassificering av belastningsattacker

För att göra de olika typerna av belastningsattacker mer överblickbara kommer följande kapitel presentera en klassifikation av dessa. Ett vanligt sätt att klassificera belastningsattacker är enligt följande fem klasser.

- **Network Device level**

  I denna klass hamnar attacker som utnyttjar svagheter eller fel i mjukvara hos nätverksutrustning och attacker som syftar till att förbruka alla resurser hos nätverksutrustning (Douligeris och Mitrokotsa, 2004). Karig och Lee (2001) beskriver ett exempel på detta där en router kör en uppsättning paketfiltreringsprocedurer. Då kan angripare överskölja denna utrustning med så många paket att den inte klarar av att filtrera alla, vilket gör att trafiken inte kan passera.

- **OS level**

  Enligt Karig och Lee (2001) hamnar attacker som utnyttjar svagheter i operativsystems protokoll här. Attacker som till exempel Ping of Death (se kapitel 2.5.1) utnyttjar protokollet ICMP.

- **Application level**

  Det finns attacker vars mål är nätverksapplikationer som körs på målsystemet. Douligeris och Mitrokotsa (2004) visar ett exempel på detta kallat Finger Bomb vilket skickar ett rekursivt meddelande till ett system som får systemet att använda rutinen finger på sig själv i en loop. Detta kan till slut förbruka systemets resurser.

- **Data flood**

  Enligt Karig och Lee (2001) fokuserar attacker i denna klass på att överskölja sina mål med stora mängder data för att antingen förbruka målets brandbredd eller att få målet att utföra stora mängder beräkningar för att behandla datan. Ett exempel på detta är Smurf-attacken (se kapitel 2.5.1).

- **Protocol feature attack**

  I denna klass hamnar, enligt Douligeris och Mitrokotsa (2004), attacker som utnyttjar svagheter hos standardprotokoll som till exempel TCP. Ett exempel på en sådan attack är SYN flood (se kapitel 2.5.2). Många av alla belastningsattacker som sker använder sig av förfalskade avsändaradresser, vilket gör det till en protocol feature attack.

2.6 Distribuerade belastningsattacker

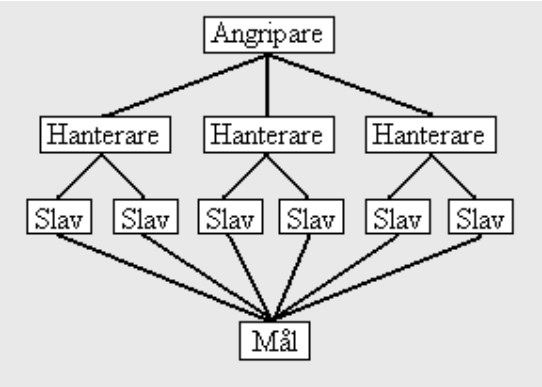
En kraftfullare uppgradering av belastningsattacker är så kallade distribuerade belastningsattacker (eng. Distributed Denial of Service attacks). Istället för att använda enbart ett system för att attackera ett annat, används många system för att utföra en samordnad attack mot ett system, vilken blir mycket kraftfullare i och med att målet för attacken belastas med ännu mer data. Lee och Specht (2003) beskriver distribuerade belastningsattacker på följande vis:

> "A Distributed Denial of Service (DDoS) attack is a large-scale, coordinated attack on the availability of services of a victim system or network resource, launched indirectly through many compromised computers on the Internet. The services under attack are those of the "primary victim", while the compromised systems used to launch to launch the attack are often called the "secondary victims". The use of secondary victims in performing a DDoS attack provides the attacker with the ability to wage a much larger and more disruptive attack, while making it more difficult to track down the original attacker." (Lee och Specht, 2003, s.1)

Som beskrivet i ovanstående citat är en belastningsattack alltså en storskalig attack vilken använder sekundära offer, vilka är skilda från det egentliga målet, för att utföra ett hårdare angrepp mot det primära offret. Användandet av de sekundära offren (även kallade slavar) gör även att angreppet är ett hot mot spårbarheten eftersom attacken inte kommer direkt från angriparen utan andra helt ovetande system.

2.6.1 Utförandet av en distribuerad belastningsattack

Figur 1 i början av detta kapitel beskrev ett vanligt förekommande problemscenario, vilket var ett angrepp av typen distribuerad belastningsattack. Hierarkin i figuren går att göra mer komplex genom att lägga till hanterare som kommunicerar med slavarna mellan angriparen och målet (se figur 7). Hanterarna läggs till för att göra vägen från angriparen till målet längre, vilket gör attacken svårare att spåra. Hanterare minskar även den trafik som angriparen behöver skicka för att inleda en attack. Det går även att ha flera nivåer av hanterare för att ytterligare förstärka dessa egenskaper.



Figur 7 - Exempel på en hierarki vid en distribueradd belastningsattack

Douligeris och Mitrokotsa (2004) beskriver förberedelsen av en distribuerad belastningsattack som en fyrstegsprocess. I steg ett väljs de slavar (eng. agents) som skall utföra attacken ut. Slavarna behöver en svaghet som gör att angriparen kan få tillgång till dem. För att utföra en så kraftfull attack som möjligt behöver de även ha ett överflöd av resurser. I steg två utnyttjas svagheten i säkerheten hos slavarna för att installera attackkoden. I detta steg försöker angriparen även skydda koden från att bli upptäckt av användaren av systemet. Under själva belastningsattacken får bara en liten del av systemets resurser, i form av till exempel bandbredd, användas så att användaren inte märker någon försämring av prestandan. Det tredje steget är ett kommunikationssteg där angriparen kommunicerar med sina hanterare för att se vilka slavar som fortfarande är aktiverade eller för att planera när attacken skall utföras. Steg fyra är det slutliga steget där attacken utförs. Angriparen kommunicerar med slavarna för att inleda attacken och skickar variabler så som målet för attacken, hur länge attacken skall pågå och andra speciella egenskaper som till exempel portnummer.

Anledningen till att dessa distribuerade belastningsattacker är så effektiva beror på Internets arkitektur. Mirkovic och Reiher (2002) menar att följande anledningar är exempel på varför dessa angrepp är så kraftfulla.

- **Resursbrist**

  Det finns en resursbrist på Internet vilket gör att användandet blir begränsat. Ett exempel på detta är om många system arbetar mot ett enda system och större resurser tillsammans än målet för angreppet.

- **Distribuerat beroende av skydd**

  En annan anledning är att det inte räcker med att ett system har bra säkerhet om de slavar som används under en attack har otillräckligt skydd, vilket gör att varje enskilt system på Internet är beroende av säkerheten hos alla andra system.

- **Address spoofing**

  Ett stort problem är avsaknaden av validering av en avsändares adress på ett IP-paket. Eftersom adressen inte valideras kan en sändare skriva in en falsk adress, vilket gör att denne blir svår att spåra vid ett angrepp av något slag samt att detta möjliggör angrepp som till exempel Smurf (se kapitel 2.5.1).

- **Distribuerad kontroll**

  Även det faktum att kontrollen av Internet är distribuerad och att de olika nätverken som bygger upp Internet körs enligt lokala föreskrifter ger problem. Detta innebär att det inte går att påtvinga globala säkerhetsmekanismer eller föreskrifter och på grund av integritetsskäl är det ofta omöjligt att granska trafik som går via flera olika nätverk som alla har olika föreskrifter.

2.6.2 Klassificering av distribuerade belastningsattacker

Distribuerade belastningsattacker klassificeras ofta enligt de fyra följande egenskaperna hos attacken.

- **Degree of automation**

Enligt Douligeris och Mitrokotsa (2004) kan denna egenskap delas upp i klasserna manuell, halvautomatisk och automatisk. De tidiga attackerna var manuella, där angriparen själv fick hitta alla slavar och installera attackkoden. Vid halvautomatiska attacker hittas lämpliga slavar automatiskt och vid automatiska attacker behöver angriparen bara skicka ett enda meddelande till en hanterare för att genomföra en belastningsattack. Resten av kommunikationen sker enbart mellan hanterare och slavar.

- **Exploited vulnerability**

Mirkovic och Reiher (2002) delar upp följande egenskap i två klasser, semantik och Brute-Force. Semantiska attacker utnyttjar svagheter i protokoll hos någon applikation som körs på målsystemet för att förbruka stora delar av dess resurser. Ett exempel på detta är SYN-flood. Brute-Force är attacker som översköljer målet med stora mängder data. Smurf-attacken är ett exempel på detta.

- **Attack rate dynamics**

Enligt Douligeris och Mitrokotsa (2004) går det även att klassificera distribuerade belastningsattacker enligt hur mycket de påverkar målet över tid. Det finns attacker som kontinuerligt attackerar målet med full kraft, men det finns även attacker som ökar sin kraft över tiden, eller varierar den beroende på målsystemets beteende.

- **Impact**

Distribuerade belastningsattacker kan enligt Mirkovic och Reiher (2002) klassificeras beroende på hur stor skada de gör på målet. Detta kan vidare delas upp i klasser huruvida systemet automatiskt kan återhämta sig från attacken eller inte. En annan egenskap är om attacken försöker avbryta systemets tillgänglighet helt och hållet, eller om den försöker att kontinuerligt förbruka en viss del av systemets resurser för att minska risken för upptäckt men ändå orsaka stora problem över tid.

3 Problembeskrivning

Användandet av Internet ökar för varje år. Bara mellan år 2000 och 2006 har användandet av Internet i världen ökat med över 200 % (Miniwatts Marketing Group, 2006). I och med det ökande användandet har dagens samhälle även blivit mer och mer beroende av de tjänster som erbjuds, till exempel e-handel, online-spel och fildelning. Vid kritiskt beroende av en sådan tjänst är det viktigt att skydda servern där tjänsten erbjuds mot attacker som hotar att rendera den otillgänglig för de tänkta användarna. Om ett företags webbserver blir otillgänglig riskerar företaget att förlora till exempel inkomst om webbservern kör en e-handelsapplikation, eller förlora ett gott rykte om de har en webbserver som tillhandahåller exempelvis support för företagets produkter/tjänster.

I kapitel två beskrevs olika former av attacker som kan förekomma mot en webbserver och en distribuerad belastningsattack visades vara den attack som är mest avancerad och svårast att skydda sitt system mot. Denna attack översköljer en webbserver med data med hjälp av många ovetande system för ökad effekt vilket kan starkt försämra eller i värsta fall helt stoppa tillgängligheten hos webbservern.

> "Extremely sophisticated, "user-friendly" and powerful DDoS toolkits are available to potential attackers increasing the danger of becoming a victim in a DoS or a DDoS attack. DDoS attacking programs have very simple logic structures and small memory sizes making them relatively easy to implement and hide." (Douligeris och Mitrokotsa, 2004, s.644)

Som citatet ovan beskriver finns det sofistikerade och kraftfulla verktyg för belastningsattacker såväl som distribuerade sådana, verktyg som har en enkel struktur och tar liten plats. Därför har ett stort antal skyddsmetoder utvecklats vilka erbjuder ett mer eller mindre bra skydd mot dessa attacker. Det stora antalet gör det dock problematiskt att enkelt kunna välja den metod som skulle vara lämpligast för en given server. För till exempel företag är det viktigt att få ett så effektivt skydd som möjligt, utan att det medför stora extra kostnader.

3.1 Problemprecisering

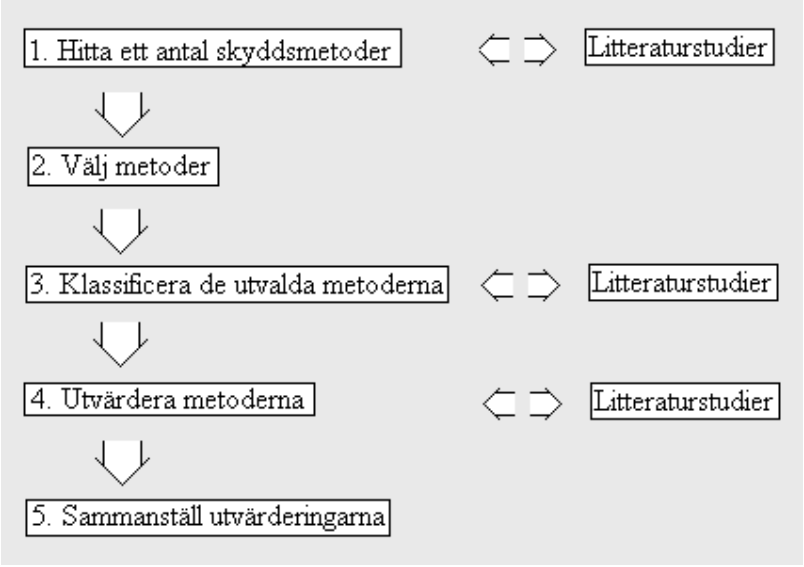
De mest använda skyddsmetoderna mot distribuerade belastningsattacker kommer att klassificeras för att sedan utvärderas med avseende på faktorer så som effektivitet, samt kostnaden för att implementera skyddet i systemet. Kostnaden för att installera och underhålla en metod är en viktig faktor eftersom så många som möjligt skall ha råd att använda den. Effektivitet hos en metod är också en mycket viktig faktor för en slutanvändare eftersom det påverkar hur säker användarens server är.

3.2 Mål

Målet är att den resulterande utvärderingen av skyddsmetoderna i denna rapport skall vara ett underlag för att avgöra vilken av dessa metoder eller kombinationer av metoder som är bäst lämpad för att appliceras på en given server.

4 Metod

För att kunna beskriva och klassificera befintliga skyddsmetoder för distribuerade belastningsattacker lämpar sig litteraturstudier bra. Den form av litteratur som kommer att fokuseras på är publicerade forskningsartiklar, vilka beskriver ovanstående metoder då dessa artiklar har granskats av experter inom området vilket gör att jämförelsen av de olika metoderna blir mer tillförlitlig, samt tekniska forskningsrapporter. Följande figur beskriver metodens relation till arbetsplanen över genomförandet av detta projekt.



Figur 8 - Relationen mellan arbetsplan och metodvad

- **Fas 1**

I fas ett kommer litteratur granskas för att samla material om så många skyddsmetoder mot distribuerade belastningsattacker som möjligt. Artiklar med brett innehåll som listar många skyddsmetoder kommer att användas här.

- **Fas 2**

Bland dessa metoder kommer sedan i denna andra fas de mest använda metoderna väljas ut.

- **Fas 3**

Litteraturstudier återkommer i fas tre där de ska användas för att klassificera de utvalda metoderna. Här kommer forskningsartiklar som fokuserar på endast en eller ett fåtal skyddsmetoder att väljas för att få en djupare insyn i varje utvald metod.

- **Fas 4**

I fas fyra kommer de utvalda metoderna utvärderas, med stöd från klassificeringen samt ytterligare litteraturstudier, med avseende på de faktorer som nämts i kapitel tre.

- **Fas 5**

I den slutliga fasen kommer de framtagna utvärderingarna sammanställas för att ge en snabbare överblick över skyddsmetoder mot distribuerade belastningsattacker.

5 Resultat

Följande kapitel inleds med en vanlig klassificering som många vetenskapliga artiklar har presenterat. Därefter följer en klassificering baserad på problempreciseringen. Till sist utvärderas metoderna som valts ut genom klassificeringen med avseende på de faktorer som beskrivits i problempreciseringen.

5.1 Vanliga klassificeringar

För att bringa struktur bland en mängd metoder brukar dessa klassificeras enligt ett antal utvalda kriterier. Några av de vanligaste klasserna som presenterats av bland andra Douligeris och Mitrokotsa (2004), Mirkovic och Reiher (2002) samt Lee och Specht (2003) visas nedan.

- **Förebyggande metoder**

  Metoder som är förebyggande (eng. preventive) försöker förhindra att en distribuerad belastningsattack kan uppstå överhuvudtaget. Detta kan ske genom till exempel filtrering av paket hos angriparens eller de sekundära målens nätverk.

- **Upptäckande metoder**

  Upptäckande (eng. detective) metoders mål är att upptäcka en pågående belastningsattack så tidigt som möjligt genom till exempel statistik över inkommande paket för att kunna starta försvarsmetoder eller varna nätverkets administratör.

- **Försvarande metoder**

  När en attack har upptäckts kan försvarande (eng. reactive) metoder användas. Exempel på hur detta kan göras är att filtrera bort paket som inte kommer ifrån vanliga användare eller att begränsa bandbredden för paketen som ser ut att komma från en angripare.

5.2 Anpassad klassificering

Det finns en stor variation hos skyddsmetoderna mot distribuerade belastningsattacker. De arbetar på olika sätt för att antingen förebygga, upptäcka eller försvara en server mot en sådan attack. De arbetar även på olika delar av nätverket mellan en angripare och ett mål, till exempel på angriparens nätverk eller på målets router.

Eftersom fokus i denna rapport ligger i att utvärdera skyddsmetoder mot distribuerade belastningsattacker för en slutanvändare med avseende på faktorer som till exempel kostnad för installation (se kapitel 3.1), kommer de vanligaste skyddsmetoderna delas upp i klasserna lokala metoder samt icke lokala metoder (se figur 9).

Lokala metoder	Icke lokala metoder
Intrångsdetekteringssystem	IP-spårning
Load balancing	ICMP-spårning
Klassbaserad köbildning	Probablistic packet marking
Stänga av oanvända tjänster	Ingress filtering
Byta IP-adress	Egress filtering
Honeypots	Förebygga sekundära mål

Figur 9 - Klassificering av skyddsmetoder

5.2.1 Lokala metoder

I denna klass placeras metoder som kan installeras på servern som skall skyddas, eller på annan utrustning inom serverns lokala nätverk. Följande metoder är vanliga metoder som kan användas inom ett lokalt nätverk.

- **Intrångsdetekteringssystem**

  Ett intrångsdetekteringssystem (eng. Intrusion Detection System) kan enligt Karig och Lee (2001) användas antingen direkt på servern som skall skyddas eller som ett separat system inom nätverket i vilket servern är lokaliserad. Ett sådant här system kontrollerar trafiken inom nätverket eller till en viss server för att upptäcka mönster som kan tyda på en attack av något slag. Den kan även känna igen till exempel Ping of Death-paket (se kapitel 2.5.1). När en potentiell attack har upptäckts kan systemet kontakta nätverkets administratör till exempel via e-post eller SMS och köra program som skyddar mot denna attack.

  Douligeris och Mitrokotsa (2004) delar in intrångsdetekteringssystemen i metoder som letar efter kända attackmönster eller metoder som letar efter anomalier i nätverkstrafiken. Attackmönstren definieras som intrångssignaturer och många populära nätverksmonitorer använder signaturbaserade metoder.

  Författarna menar vidare att de metoder som letar efter anomalier gör statistiska analyser av nätverkspaket. Detta kan vara till exempel analys av header-information hos paket som når en server eller av paket- och routingstatistik som hämtas från en router. En annan metod är att analysera paket som tappats på grund av en överbelastning hos nätverkskomponenten. Om en statistisk anomali upptäcks bland dessa paket kan routern meddelas och börja filtrera bort dessa paket.

- **Load balancing**

Enligt Karig och Lee (2001) kan replikeras många hårt belastade webbservrar för att dela upp belastningen av normal trafik. De replikerade servrarna kan placeras på olika platser för att vara närmare olika användare. De används tillsammans med en så kallad Load Balancer, vilken fördelar trafiken mellan de replikerade servrarna. Detta gör även att effekten av en belastningsattack minskas.

- **Klassbaserad köbildning**

Köbildningsmetoder används, enligt Douligeris och Mitrokotsa (2004), ofta för att bekämpa distribuerade belastningsattacker. Den mest använda metoden är den klassbaserade köbildningen (eng. Class-based queuing). Denna metod delar upp inkommande paket i olika klasser, baserat på vilken typ av paket det är.

Kargl, Maier och Weber (2001) visar att denna metod till exempel finns inbyggd i Linux kernel. Här kan klasserna sedan tilldelas olika stor bandbredd och om en kö blir full slängs paketen.

- **Stänga av oanvända tjänster**

Att stänga av tjänster som inte används hos en server som till exempel character generator (se kapitel 2.5.1) förhindrar enligt Douligeris och Mitrokotsa (2004) att dessa kan användas vid en belastningsattack.

- **Byta IP-adress**

Douligeris och Mitrokotsa (2004) visar att genom att byta serverns IP-adress till en ny kommer alla routrar på Internet till slut ha blivit uppdaterade och kommer då att kasta alla paket med den gamla adressen, vilket gör att en pågående attack kommer att avbrytas.

Enligt Kargl, Maier och Weber (2001) kan det ta ett antal dagar innan alla DNS-servrar är uppdaterade, vilket gör servern är otillgänglig för vanliga användare. Detta är oacceptabelt eftersom effekten av det är lika negativ för servern som från vilken belastningsattack som helst. Ett ytterligare problem är att attackprogrammen kan innehålla funktionalitet som kontaktar DNSer för att få den nya IP-adressen till servern.

- **Honeypots**

Douligeris och Mitrokotsa (2004) beskriver en så kallad honeypot som en server med begränsad säkerhet, vilken skall dra till sig uppmärksamheten från en angripare. Detta skall då leda uppmärksamheten bort från den primära servern som skall skyddas. Honeypot-servern loggar och analyserar även eventuella attacker för att kunna förhindra att de sker på den primära servern.

5.2.2 Icke lokala metoder

I denna klass placeras de övriga metoderna, det vill säga de metoder som installeras på utrustning som befinner sig utanför serverns lokala nätverk. Dessa metoder innebär ofta att paket görs spårbara (se kapitel 2.1.4, 2.3.2 samt 2.3.3) eller att paket filtreras bort innan de lämnat en angripares nätverk. Följande metoder är exempel på vanliga sådana metoder.

- **IP-spårning**

  Enligt Douligeris och Mitrokotsa (2004) används IP-spårning (eng. IP traceback) när en attack upptäckts för att spåra paketen bakåt mot ursprunget. Målet med denna metod är att identifiera angriparen samt upptäcka asymmetriska rutter på Internet. Problemet med detta är dock att Internets rutter är tillståndslösa (eng. stateless) samt att det sker manuellt; administratören på nätverket som attackeras kontaktar nätverkets ISP för att få reda på varifrån paketen kommer.

- **ICMP-spårning**

  För att spåra en angripare kan, enligt Douligeris och Mitrokotsa (2004), ICMP-spårning användas. Med denna metod skickar en router ett ICMP-spårningspaket till mottagaren. Detta paket genereras slumpmässigt, när ett vanligt paket passerar routern, med en sannolikhet på cirka ett av 20000 paket. Om tillräckligt många sådana paket fanns samlade hos en server som blir attackerad skulle en kedja av dessa spårningspaket kunna skapas för att hitta angriparen. För att denna metod skall fungera krävs att alla routrar implementerar den. Ett annat sätt är att skicka spårningspaketen tillbaka till avsändaren. Ett problem är dock att det skapas extra trafik mellan routrarna.

- **Probabilistic packet marking**

  Douligeris och Mitrokotsa (2004) visar att i denna metod kodas en del av paketets tidigare rutt (eng. route) in i varje IP-paket som passerar en router. På så vis går det enkelt att spåra en angripare. Fördelen med denna metod är att den inte skapar någon extra trafik men istället behöver varje router utföra mer beräkningar för varje paket som passerar. Denna metod för att spåra en angripare kan användas både efter och medan en attack utförs. Ytterligare en fördel är att ingen ISP behöver kontaktas i spårningsprocessen.

- **Ingress filtering**

  Vid många belastningsattacker används address spoofing (se kapitel 2.3.2). För att förhindra detta kan, enligt Douligeris och Mitrokotsa (2004), en ISP (Internet Service Provider) använda en filtreringsmetod kallad Ingress (inkommande) filtering på sin router. Den filtrerar bort paket med förfalskade avsändaradresser från att komma in i det egna nätverket genom att kontrollera om IP-adressen matchar domänprefixet från det anslutande nätverket.

- **Egress filtering**

Karig och Lee (2001) beskriver en annan filtreringsmetod, kallad Egress (utgående) filtering, som kan användas på en ISPs routrar. Om ett paket försöker lämna ISPns nätverk genom en sådan router men har en förfalskad avsändaradress som ligger utanför detta nätverk kommer routern att filtrera bort och logga detta paket. Ett nätverk som använder sig av en sådan filtreringsmetod blir då mindre attraktivt att använda som bas för att utföra belastningsattacker från.

- **Förebygga sekundära mål**

Om en angripare hindras från att använda sekundära mål (se kapitel 2.6.1) för sina attacker har denne enligt Lee och Specht (2003) inget nätverk att utföra sin distribuerade belastningsattack från. Ett sekundärt mål kan skyddas från att användas som slav i en attack genom att installera skydd mot Trojaner och virus, och hålla dessa skyddsprogram uppdaterade samt uppdatera säkerhetspatcher för till exempel operativsystemet och webbläsare.

5.3 Utvärdering av metoderna

I följande kapitel kommer de skyddsmetoder som befinner sig i klassen lokala metoder utvärderas. Enbart denna klass har valts eftersom metoderna som befinner sig här kan installeras och användas av en slutanvändares server eller nätverk. Följande metoder är de som kan användas av en slutanvändare. Varje metod utvärderas med avseende på kostnaden för att installera metoden samt hur effektiv den är.

- **Intrångsdetekteringssystem**

Kostnaden för denna metod beror på huruvida metoden är implementerad på servern som skall skyddas eller som ett separat system inom nätverket. Kostnaden blir naturligtvis mindre om den implementeras på servern eftersom ett nytt system inte behöver köpas in. Men den skulle ta resurser från servern för att utföra analyser av de inkommande paketen vilket kan leda till försämrad prestanda för servern. Detta i sin tur leder till att servern kan behöva uppgraderas vilket också medför en viss kostnad. Ett intrångsdetekteringssystem är effektivt för att upptäcka en pågående attack.

- **Load balancing**

Själva systemet som fördelar trafiken behöver inte vara speciellt dyrt, men att replikera en server i ett antal nya instanser innebär en stor kostnad. Eftersom denna metod inte försöker förhindra en belastningsattack utan enbart sprider ut den på alla tillgängliga servrar kan den anses som mindre effektiv.

- **Klassbaserad köbildning**

En metod som denna kan med lätthet implementeras hos en server. I Linux kernel finns den till exempel redan inbyggd. Detta leder till en låg kostnad. En klassbaserad köbildning kan vara mycket effektiv om klassificering av paket lyckas.

- **Stänga av oanvända tjänster**

Att stänga av oanvända tjänster innebär ingen extra kostnad mer än att konfigurera servern. Att stänga ner oanvända tjänster som kända distribuerade belastningsattacker utnyttjar är mycket effektivt, men förhindrar bara specifika attacker. Det innebär inget skydd mot resterande attacker och det är inte heller alltid möjligt att stänga ner tjänster eftersom de kan vara nödvändiga att köra.

- **Byta IP-adress**

Att byta en IP-adress innebär ingen märkvärd kostad. Denna metod avbryter en belastningsattack mot en server, men hindrar även vanliga användare att komma åt den.

- **Honeypots**

Att installera honeypot-servrar innebär en relativt hög kostnad utan att ge en garanti att de är systemen som blir attackerade, istället för servern som skall skyddas. Om de lyckas locka en angripare är de effektiva, men om en attack har påbörjats mot servern som skall skyddas har de ingen effekt.

5.4 Betygsättning av metoderna

I följande kapitel sammanställs utvärderingen av metoderna i föregående kapitel enligt följande system. Varje metod har tilldelats ett betyg från ett till fem för varje jämförelsefaktor. För kostnad innebär betyget ett att metoden är dyr att installera medan fem i betyg innebär att den medför en låg kostnad. För effektivitet innebär ett högt betyg att metoden är erbjuder ett effektivt försvar mot distribuerade belastningsattacker.

- **Intrångsdetekteringssystem**

Eftersom den befintliga servern måste uppgraderas eller en extra server köpas in medför den en viss extra kostnad. Betyget blir därför 3. Ett intrångsdetekteringssystem är mycket effektivt för att upptäcka en pågående attack, således blir betyget för effektivitet 5.

- **Load Balancing**

Det innebär en mycket stor kostnad att köpa in ett antal nya servrar, därför ges betyget 1. Load Balancing kan vara mycket effektivt för att minska skadan vid en attack, men eftersom den inte motverkar attacken utan endast fördelar den på fler servrar, tilldelas metoden bara betyget 4.

- **Klassbaserad köbildning**

Eftersom klassbaserad köbildning med enkelhet kan köras på servern som skall skyddas och endast en uppgradering krävs ges betyget 4 i kostnad. Om metodens klassificering lyckas är detta en mycket effektiv metod att motverka en attack. Därför blir betyget 5.

- **Stänga av oanvända tjänster**

Att stänga av tjänster medför ingen kostnad, vilket ger betyget 5. Eftersom bara vissa specifika attacker hindras med hjälp av detta, och eftersom alla tjänster inte går att stänga av blir betyget i effektivitet endast 2.

- **Byta IP-adress**

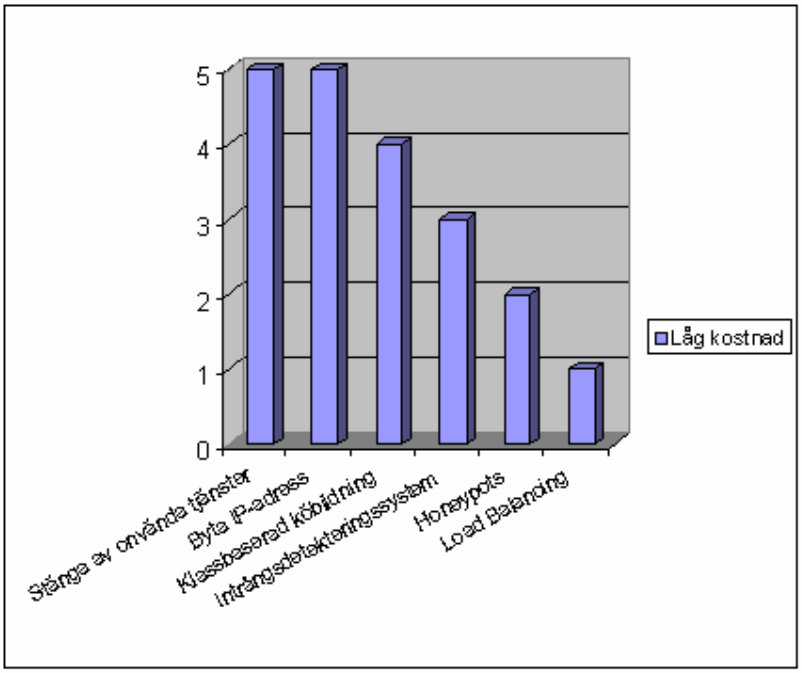
Byte av IP-adress medför heller ingen nämnvärd kostnad. Betyget 5 i kostnad ges således. Att byta IP-adress förhindrar alla paket att nå servern, både attackpaket och paket från vanliga användare. Eftersom servern blir otillgänglig för de vanliga användarna kan denna metod ses som helt ineffektiv och får således 1 i betyg.

- **Honeypots**

Att installera honeypots innebär alltid en relativt hög kostnad då ny servrar som skall agera lockbete måste köpas in. Därför ges betyget 2. Eftersom denna metod endast är effektiv om angriparen råkar välja denna istället för servern som skall skyddas erbjuder den inte ett tillräckligt effektivt skydd och får enbart 2 i betyg.

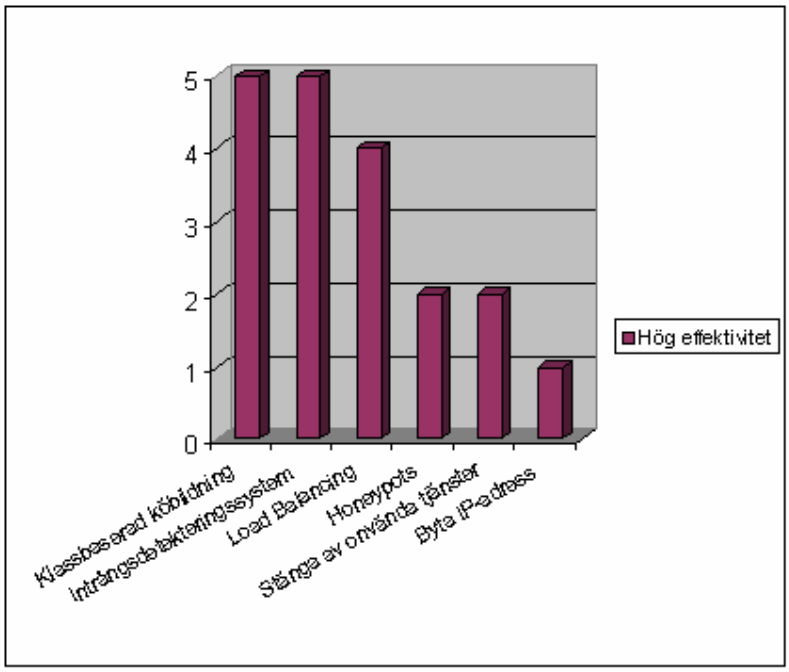
5.5 Sammanställning av betygen

I följande kapitel sammanställs de betyg som sattes i föregående kapitel.



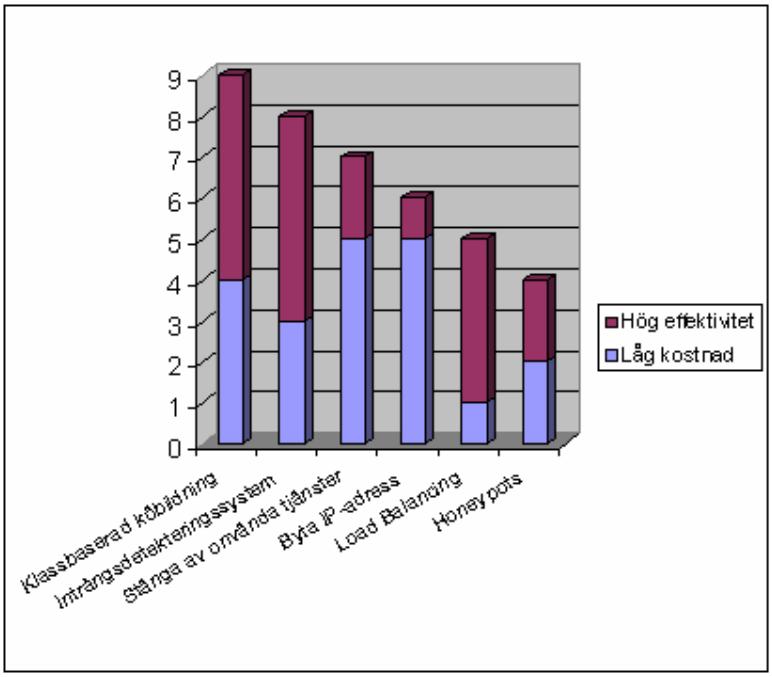
Figur 10 - Kostnad

I figur 10 jämförs metodernas betyg för hur låg kostnaden för att implementera respektive metod är.



Figur 11 - Effektivitet

I figur 11 jämförs metodernas betyg för hur effektivt skydd respektive metod erbjuder mot distribuerade belastningsattacker.



Figur 12 – Betygssammanställning

I figur 12 summeras betygen för varje metod för att ge en bild över hur bra metoderna är i förhållande till varanda med avseende på kostnad och effektivitet. Summeringen innebär att det slutliga betyget kan sträcka sig från två till och med tio, där tio är ett bra betyg och två är dåligt. Det högsta totala betyget får metoden klassbaserad köbildning medan Honey Pots får det lägsta.

6 Slutsats

I detta projekt har målet varit att klassificera och utvärdera de vanligaste skyddsmetoderna mot distribuerade belastningsattacker. Tolv metoder valdes ut och klassificerades i två klasser; lokala metoder och icke lokala metoder. De sex metoder som klassificerades som lokala metoder utvärderades enligt faktorerna kostnad och effektivitet.

Eftersom betygen är satta enbart utifrån deras beskrivningar skall dessa främst ses som riktlinjer vid en jämförelse. Klassbaserad köbildning vilket fick nio i betyg, och intrångsdetekteringssystem fick åtta. Likheten i betyg mellan de två metoderna gör det svårt att säga vilken metod som är bäst. Dock kan dessa två metoder jämföras med till exempel metoden Honey Pots, vilken enbart fick 4 i betyg. Här är skillnaden i betyg stor och det kan sägas med relativt god säkerhet att metoderna klassbaserad köbildning samt intrångsdetekteringssystem är bättre än metoden Honey Pots.

Om metoder kombineras visar resultatet att en kombination av klassbaserad köbildning och intrångsdetekteringssystem är att föredra. För att minimera kostnaden kan dessa två metoder köras på samma server som den som skall skyddas, med lämpliga uppgraderingar.

6.1 Framtida arbete

Eftersom nya belastningsattacker upptäcks och skyddsmetoder mot dessa utvecklas, skulle denna rapport behöva uppdateras genom att inkludera dessa metoder.

De faktorer som metoderna i resultatet utvärderades med avseende på skulle kunna utökas. Exempel på sådana faktorer skulle kunna vara hur lätt en metod är att installera samt administrera eller vilka systemkrav som krävs för att metoden skall kunna köras.

Metoderna skulle även kunna implementeras för att själv kunna testa dem enligt de utvalda utvärderingskriterierna.

7 Diskussion

För att utvärdera skyddsmetodernas effektivitet har endast litteraturstudier använts. Det innebär att resultatet i denna rapport är beroende av riktigheten hos mätningarna av effektiviteten i den litteratur som studerats. En komplementerande metod skulle vara implementation. Skulle metoderna implementeras och testas skulle det innebära en större säkerhet att resultatet i denna rapport är korrekt.

Istället för att själv ha utfört betygsättningen kunde ett antal kunniga personer inom området fått göra var sin individuella betygsättning. Ett medelvärde av dessa betygsättningar skulle sedan ha presenterats som resultat, vilket skulle vara mer trovärdigt.

En annan faktor som kan ha påverkat resultatet i denna rapport är det betygsystem som valts för utvärderingen av skyddsmetoderna. Hade betygen sträckt sig från till exempel ett till tre, eller ett till tio kunde resultatet ha sett annorlunda ut.

De jämförelsefaktorer som valdes för utvärderingen var kostnad och effektivitet. Dessa är mycket viktiga för valet av en metod, men det finns dock andra viktiga faktorer som också kunde ha tagits hänsyn till, till exempel installerbarhet och administrerbarhet. Detta kunde ha gjort att resultatet över vilka metoder som var bäst blivit annorlunda.

Vid sammanställningen av det sammanlagda betyget för varje metod väger kostnaden och effektiviteten lika tungt. Detta har gjort att metoden byta IP-adress har fått hela sex i betyg, trots att den aldrig skulle väljas att implementeras på grund av sin obefintliga effektivitet. Istället kunde effektiviteten till exempel fått en dubblerad betygskala, vilket skulle göra effekten av kostnaden på slutresultatet mindre.

Den anpassade klassificeringen som presenterades i kapitel 5.2 underlättade utvärderingen av metoderna eftersom den klassificerade bort oväsentliga skyddsmetoder, det vill säga metoder som inte kan implementeras på det lokala nätverket eller servern.

Referenser

Douligeris, C. & Mitrokotsa, A., 2004. DDoS attacks and defense mechanisms: classification and state-of-the-art. *Computer Networks: The International Journal of Computer and Telecommunications Networking*, 44(5), April, s. 643-666

Gregfelt, B., 2005. *Svenska Antipiratbyrån* [online]. Tillgänglig från: http://www.antipiratbyran.com/index.htm?id=wrk [Nedladdad 14e augusti 2006].

Kargl, F., Maier, J. & Weber, M., 2001. Protecting web servers from distributed denial of service attacks. *Proceedings of 10th international WWW conference 2001.* s. 514-524

Karig, D. & Lee, R., 2001. Remote Denial of Service Attacks and countermeasures. Department of Electrical Engineering, Princeton University. October. Technical Report CE-L2001-002.

Lee, R. & Specht, S., 2003. Taxonomies of Distributed Denial of Service Networks, Attacks, Tools, and Countermeasures. Department of Electrical Engineering, Princeton University. May. Technical Report CE-L2003-03.

Lindstedt, U., 2005. *Antipiratbyrån sänkta av uppretade pirater* [online]. Tillgänglig från: http://www.idg.se/ArticlePages/200503/07/20050307143936_IW/20050307143936_IW.dbp.asp [Nedladdad 14e augusti 2006].

Miniwatts Marketing Group, 2006. *World Internet Usage Statistics and Population Stats* [online] Tillgänglig från: http://www.internetworldstats.com/stats.htm [Nedladdad 14 augusti 2006].

Mirkovic, J. & Reiher, P., 2002. A taxonomy of DDoS attacks and DDoS defence mechanisms. UCLA CSD, Technical Report no. 020018.

Pfleeger, C. P. 2003. *Security in Computing*. 3rd edition. Prentice