HÖGSKOLAN SKÖVDE

Institutionen för kommunikation och information
Examensarbete i datalogi med inriktning mot nätverks- och systemadministration
15hp
C-nivå
Vårterminen 2010

Genomgång av skyddsmetoder för TCP SYN flooding

Jonatan Thorstensson

HÖGSKOLAN SKÖVDE

Institutionen för kommunikation och information
Examensarbete i datalogi med inriktning mot nätverks- och systemadministration
15hp
C-nivå
Vårterminen 2010

Genomgång av skyddsmetoder för TCP SYN flooding

Examensrapport inlämnad av Jonatan Thorstensson till Högskolan i Skövde, för Kandidatexamen (B.Sc.) vid Institutionen för kommunikation och information. Arbetet har handletts av Helen Pehrsson.

2010-06-04

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: _____

SYN flooding

Jonatan Thorstensson

Abstrakt

Följande arbete behandlar möjliga lösningar för hantering av SYN flooding, en Denial-of-Service-attack mot tjänster som använder TCP för kommunikation över datanätverk. Ett flertal olika skyddsmetoder, med varierande ansatser, identifieras, beskrivs och undersöks. Även möjligheter att kombinera dessa analyseras. Det visas att genom att implementera existerande skydd, samt kombinera flera av dessa begränsas hotet från SYN flooding avsevärt. Rekommendationer presenteras dessutom för hur organisationer bör gå tillväga för att säkra tjänster som riskerar att utsättas för SYN flooding-attacker genom att implementera skydd nära tjänsten först samt därefter ytterligare lager allt längre ut i nätverket.

Nyckelord: SYN flooding, Denial of Service, rekommendationer, skydd

Innehållsförteckning

1 Introduktion

SYN flooding är det namn som används för att beskriva en Denial of Service (DoS)-attack vilken använder sig av en svaghet i Transmission Control Protocol (TCP). Problemet uppdagades i stor skala under 1996 då, efter att kod för att genomföra en SYN flooding-attack publicerats på flera välkända hacker-nätverk, en amerikansk internetleverantörs mail-tjänst blockerades ut av en sådan attack (Internet Engineering Task Force, 2007).

Hansson (2010) rapporterar att företaget Västgöta-Data AB utsätts för ungefärligen två attacker per månad vilka omöjliggör internetaccess under cirka en halvtimme per incident. Detta innebär för företaget, med sina 8 anställda, en årlig förlust på närmare 20 000 kronor, eller en förlust av potentiell vinst på dryga 60 000 kronor.

En exakt bild för hur hårt drabbade svenska organisationer är av DoS-attacker i allmänhet eller SYN flooding i synnerhet är inte helt enkelt att göra sig. Utgångspunkten för arbetet bakom denna rapport är dock att sådana attacker sker på en inte obetydlig skala, och intresse bör således finnas för ett effektivt skydd för att hantera dessa.

TCP är en grundläggande komponent i den välanvända TCP/IP-protokollsviten, vilken är dominant på Internet idag. En stor mängd applikationsprotokoll använder helt eller delvis TCP för kommunikation över datanätverk (Halsall, 2005). Rollen TCP har i denna svit är att erbjuda pålitlig dataöverföring genom att tillämpa flödeskontroll och att skicka om förlorade segment. För att kunna erbjuda dylika tjänster krävs att en förbindelse sätts upp mellan kommunicerande parter så att inkommen data därefter kan härledas till en sådan förbindelse. Genom att använda sekvensnummer kan protokollet upptäcka om något datasegment förlorats på vägen för att då skicka om detta (Internet Engineering Task Force, 1981).

TCP agerar på transportlagret i den protokollstack som används på Internet. Andra protokoll på samma lager kan användas i TCP:s ställe för att undvika SYN flooding. Generellt finns ett alternativt protokoll, User Datagram Protocol (UDP). UDP saknar dock stöd för pålitlig dataöverföring, vilket är det utmärkande draget för TCP, och kan därmed inte nöjaktigt överföra data i fall där det är av stor vikt att överförd data är korrekt (Internet Engineering Task Force, 1980). Det betydligt mer nytillkomna protokollet Stream Control Transmission Protocol (SCTP) har stöd för pålitlig överföring samtidigt som inbyggt skydd mot attacker mot sessionsetablering finns (Internet Engineering Task Force, 2000b). En övergång till ett sådant protokoll skulle dock med stor sannolikhet kräva stora omställningar och kan antas vara mycket kostsam. En mjukvara vilken klarar av att hantera SYN flood-attacker vid fortsatt användning av TCP kan därmed antas vara av ekonomiskt intresse.

Motiveringen bakom skapandet av TCP var behovet av pålitlig överföring. Pålitlig i avseendet att kunna garantera att data når målet, utan att skadas eller försvinna på vägen. I en nätverksmiljö tämligen olik dagens tycks tankar kring motståndskraft mot DoS-attacker saknats. Detta inte helt obefogat då protokollet TCP i den version som används idag standardiserades redan år 1981 medan den svaghet som ligger till grund för SYN flooding-attacker inte uppdagades förrän tretton år senare, 1994, och kod för att genomföra en sådan attack först publicerades på bred front ytterligare två år senare, 1996 (Internet Engineering Task Force, 2007).

Mer specifikt ligger svagheten i hur sessioner startas i TCP. Attacken genomförs så att angriparen öppnar en avsevärd mängd sessioner genom att skicka en stor mängd SYN-segment mot den tjänst som attackeras. Detta utan att slutföra den trevägshandskakning som används för uppsättandet av sådana, det vill säga utan att svara med ett ACK-segment på det SYN/ACK-segment som skickas av offret. Offrets så kallade *backlog*-buffert fylls då helt, varpå samtliga nyinkomna förfrågningar nekas, såväl legitima som från angriparen. Genom att fortsätta skicka falska förfrågningar kan därefter angriparen omöjliggöra legitima förbindelser under en godtyckligt lång tid om attacken inte på något vis stoppas (Cohen, 1996). Attacken består således av en flod, på engelska flood, av SYN-segment.

I attackdefinitionen ingår dessutom att samtliga SYN-segment som skickas har en förfalskad, eller *spoofad* avsändar-IP-adress. Detta då adressen till vilken offret skickar sitt SYN/ACK-segment, för en lyckad attack, ej kan vara i bruk. En bieffekt är att attacken, på grund av det förbindelselösa beteendet hos IP, dessutom blir svår att spåra.

De falska segment som mottags av offret bidrar till vad som kallas halvöppna sessioner. Ett halvöppet tillstånd innebär att servern har reserverat resurser för att lagra information om den förbindelse som förväntas etableras med den maskin från vilken SYN-segmentet mottagits. Då resurser är finita måste en gräns etableras för maximalt antal simultana halvöppna sessioner. Innan problemet med SYN flooding uppdagades var denna gräns satt mycket lågt, ofta kunde så lite som 6-10 halvöppna sessioner hanteras innan backlogen var full. Att släppa på begränsningen för maximalt antal halvöppna sessioner skulle naturligtvis utrota problemet med SYN flooding som det ser ut idag, men samtidigt öppna dörrarna för möjligheten att genom att öppna ett stort antal halvöppna sessioner uttömma samtliga resurser hos servern, vilket skulle resultera i en än värre DoS-attack (Harris & Hunt, 1999).

Detta arbete syftar till att genom att analysera befintliga metoder för att skydda tjänster mot SYN flooding kunna utvärdera olika möjliga lösningar samt undersöka möjligheter att kombinera flera befintliga skydd för att mer effektivt kunna skydda kritiska tjänster, utan att för den delen överge TCP som transportprotokoll.

Det finns i dagsläget inga standardiserade lösningar på problemet med SYN flooding trots att detta kan antas vara en vanlig metod för genomförande av DoS-attacker. Sedan 1996 då problemet på bred front uppmärksammades har dock diverse skyddsmetoder tagits fram (Internet Engineering Task Force, 2007). Dessa har vitt skilda sätt att angripa problemet, och därför har ett urval gjorts av skyddsmetoder vilka kommer analyseras.

2 Bakgrund

Nedan följer beskrivningar av koncept relevanta för förståelse av hur en SYN flooding-attack går till. Beskrivs görs vilka protokoll som utnyttjas och hur de missbrukas för att genomföra en attack.

2.1 Denial of Service (DoS)

Denial of Service-attacker syftar till att genom överbelastning av en tjänst med icke-legitima förfrågningar eller trafik kunna rendera tjänsten otillgänglig för legitima användare. En DoS-attack behöver inte nödvändigtvis skada resurser permanent, utan syftar till att under en tid skada tillgängligheten för denna. De vanligaste typerna av DoS-attacker är de som riktas mot bandbredd på nätverket eller uppkopplingsmöjligheter för en tjänst. Legitima förfrågningar och trafik dränks ut genom en stor mängd av falska sådana (Douligeris & Mitrokotsa, 2004).

Generellt delas DoS-attacker upp i två olika generella grupper, en vilken syftar till att otillgängliggöra en tjänst genom att utnyttja överlägsna resurser och en andra vilken skapar mer skräddarsydda paket för att utnyttja problem i protokoll eller applikationer. Den förstnämnda kategorin är svårare att skilja från normal, legitim, trafik. Den sistnämnda har dock större effekt i förhållande till förbrukade resurser hos angriparen.

2.1.1 Distributed Denial of Service (DDoS)

Då en DoS-attack utförs simultant från flera punkter i nätverket kallas detta för en distribuerad attack, engelska distributed. Generellt gäller att en angripare, ofta med hjälp av ett mellanlager av så kallade *masters* eller *handlers*, styr en stor mängd infekterade datorer, så kallade *zombier*, vars ägare inte är medvetna om att de medverkar i en DDoS-attack. DDoS-attacker är mer förödande än vanliga DoS-attacker främst då den sammanlagda mängden resurser som innehas av angriparen är större, men även på grund av faktorer som att de anfallande zombierna generellt är utspridda över nätverket. Det innebär med andra ord att attacken inte kan avskärmas genom att blockera trafik från en viss maskin eller ett visst nätverk eller nätverkssegment. Det är dessutom mer problematiskt att spåra vem som kontrollerar de anfallande maskinerna (Douligeris & Mitrokotsa, 2004).

2.2 Internet Protocol (IP)

IP används för adressering av paket skickade över datanätverk. I varje skickat IP-paket finns två adresser; en mottagare och en avsändare. Samtliga svar på mottagna paket skickas således till avsändaren för det paket som svaret avser. Detta kallas för ett förbindelselöst beteende. Alternativet hade inneburit att en förbindelse hade etablerats till vilken inkommen trafik kunde associeras, samt svar kunde skickas till motparten i denna förbindelse. IP överlämnar dock sådan funktionalitet åt andra protokoll, i aktuella fall TCP (Halsall, 2005).

2.2.1 IP spoofing och SYN flooding

Spoofing är en engelsk term som innebär att något imiteras. I sammanhanget IP innebär termen att avsändaradressen ändras från den riktiga till någon annan. IP spoofing ligger till grund för SYN flood-attacker genom att adresser som spoofas av angriparen är sådana denne kan vara tämligen säker på är routbar, det vill säga nätverket adressen tillhör är nåbart, men att någon maskin som svarar på den inte existerar. Då TCP svarar på ett SYN-segment sänt från en sådan adress kommer det genererade SYN/ACK-segment resultera i att ett felmeddelande via Internet Control Message Protocol (ICMP) av typen *destination unreachable* mottas hos offret. TCP anser detta fel irrelevant och lämnar lösningen åt underliggande protokoll, det vill säga IP. Då ingen maskin existerar som IP kan nå lämnas problemet olöst. Om däremot en maskin finns som svarar på den spoofade adressen kommer denna att då den mottager ett SYN/ACK-segment som den inte efterfrågat svara med ett RST-segment vilket återställer sessionen (Harris & Hunt, 1999).

IP spoofing innebär inte bara att en angripare kan avgöra vart SYN/ACK-segment skall skickas utan ger även ett utmärkt kamouflage, då det enda enkla sättet att känna till avsändaren av ett paket är att inspektera avsändaradressen. Detta beror på att IP arbetar utan att först etablera en förbindelse mellan ändpunkterna för kommunikationen. Xiao et al. (2008) talar om möjliga metoder för att avgöra faktiskt ursprung av spoofade paket. Metoder för att undersöka detta, exempelvis den presenterad av Internet Engineering Task Force (2000a), kräver delaktighet av flera eller samtliga routers på nätverket som de spoofade paketen skickas över. Dessa koncept faller dock utanför omfattningen av detta arbete.

2.3 Transmission Control Protocol (TCP)

Protokollet TCP är ett förbindelseorienterat protokoll för tillförlitlig överföring av data. Protokollet tillsammans med övriga protokoll i TCP/IP-modellen utgör grunden för Internet. En stor mängd applikationsprotokoll använder TCP för att pålitligt överföra data.

För att de noder som kommunicerar ska kunna kontrollera att den data som skickats från avsändaren mottagits oförändrad och i sin helhet hos mottagaren måste en förbindelse sättas upp. Innan en överföring startar sätter TCP upp en session mellan de två kommunicerande parterna. Sessionen etableras genom en så kallad trevägshandskakning, vilket innebär att om en nod A önskar kommunicera med en nod B skickas en förfrågan om att öppna en session genom att ett meddelande med flaggan SYN satt skickas tillsammans med ett sekvensnummer SEQ, som identifierar sessionen samt meddelandeordning inom denna. När detta meddelande tas emot hos nod B öppnas sessionen halvt och ett svar med SYN-flaggan samt en bekräftelseflagga ACK satta och ACK-nummer satt till mottaget SEQ ökat med ett, för att indikera att bekräftelsen gäller den SYN som mottagits, skickas tillbaka. Detta svar innehåller dessutom ett nytt SEQ för att identifiera och ordna meddelanden skickade i denna riktning. När nod A mottar detta meddelande försätts den i ett tillstånd där sessionen är etablerad, och svarar nod B med ett bekräftelsemeddelande med flaggan ACK satt, och ACK-nummer satt till mottaget SEQ ökat med ett. SEQ och ACK används sedan under fortsatt kommunikation för att säkerställa att skickad data mottagits vid mottagarnoden (Internet Engineering Task Force, 1981).

TCP A			TCP B
1. CLOSED			LISTEN
2. SYN-SENT -->	<SEQ=100> <CTL =SYN>	-->	SYN-RECEIVED
3. ESTABLISHED <--	<SEQ=300> <ACK=101> <CTL=SYN,ACK>	<--	SYN-RECEIVED
4. ESTABLISHED -->	<SEQ=101> <ACK=301> <CTL=ACK>	-->	ESTABLISHED

Motsvarande för nedkoppling av en session skickas från någon part ett FIN-segment, på vilket den andra parten svarar FIN och ACK, vartefter den första parten svarar med ett slutgiltigt ACK (Internet Engineering Task Force, 1981).

I händelse av fel, det vill säga om någon av de kommunicerande parterna tar emot ett meddelande vilket inte kan stämmer överens med det tillstånd denne är i, skickas ett RST-segment för att omedelbart återställa förbindelsen (Internet Engineering Task Force, 1981).

2.3.1 SYN flooding som DoS-attack

Av de två kategorier av DoS-attacker som presenteras i kapitel 2.1 tillhör SYN flooding den senare, då den utnyttjar ett problem i ett protokoll genom att skicka problematisk trafik. Trots detta är den mycket svår att upptäcka då en inkommande attack är närmast identisk med en stor mängd legitim trafik. Det enda som skiljer är att de synbara avsändarna inte existerar. Trots att attacken kräver manipulation av paket på bitnivå är den inte särskilt praktiskt svår att genomföra. Färdiga verktyg, så som *hping* finns enkelt tillgängliga på Internet för vem som helst att använda.

Som DoS-attack är SYN flooding mycket effektivt. Då problemet var nyupptäckt och många tjänster fortfarande helt utan skydd kunde en vanlig användare på ett fåtal sekunder genomföra en förödande attack (Cohen, 1996). Utförd som DDoS är attacken inte bara mer kraftfull i mängd inkommande SYN-paket utan dessutom otroligt svår att spåra.

2.4 Tidigare arbeten inom området

De tidigare arbeten på området som identifierats tycks samtliga presentera nya skyddsmetoder (Xaio et al., 2007; Schuba et al., 1997; Tupakula et al., 2004; Wang et al., 2002a; Wang et al., 2002b; Lemon, 2002; Ohsita et al., 2005, Safa et al., 2007), förbättringar av tidigare skyddsmetoder (Zuquete, 2002), eller en översikt av DoS-attacker (Douligeris & Mitrokotsa, 2003; Harris & Hunt, 1999). Testning är en del i flera av dessa arbeten, där den nya presenterade skyddsmetoden ställs emot någon annan i något scenario. Det tycks dock saknas en genomgång av ett något större antal skyddsmetoder. Safa et al. (2007) presenterar flera olika skyddsmetoder, men testar endast den egna samt en ytterligare.

Detta arbete syftar till att sammanställa de arbeten som gjorts samt jämföra dessa för att organisationer enklare skall kunna identifiera skyddsmetoder vilka är kompatibla med deras system samt effektivt kan skydda tjänster mot SYN flooding-attacker. Något tidigare arbete som fyllt detta syfte har inte kunnat hittas.

3 Problembeskrivning

Detta arbete syftar till att efter följande tes granska olika metoder för att skydda tjänster mot SYN flooding-attacker:

"genom att undersöka existerande skyddsmetoder kan rekommendationer ges till organisationer i riskzonen för hur dessa kan utnyttja och kombinera dessa för att effektivare upptäcka, motverka och lindra effekterna av SYN flooding-attacker" .

Skyddsmetoder som skall undersökas väljs ut för att i mesta möjliga mån vara representativa för de olika kategorier av skydd som används idag enligt kategoriseringar så som den presenterad av Internet Engineering Task Force (2007), kompletterat vid behov. Genom att undersöka dessa metoder samt ta i åtanke vilken kategori de tillhör bör slutsatser kunna dras kring huruvida en kombination av olika metoder kan användas för ökad effektivitet.

Förhoppning finns om att detta kan bidraga till att organisationer, som Västgöta-Data AB, vilka lider ekonomiska förluster till följd av SYN flooding-attacker enklare skall kunna hitta ett anpassat skydd för att upptäcka, motverka och lindra dessa. Det antas att Västgöta-Data AB inte är ensamma om att utsättas för DoS-attacker baserade på SYN flooding, då trots deras internetbaserade programvarudistribution, företaget inte kan sägas vara ett högriskmål. Organisationer vilka är ständigt inblandade i kontroversiella frågor, exempelvis politiska partier eller intresseorganisationer, där klara hotbilder kan finnas från externa källor är sannolikt än mer utsatta. Detsamma gäller organisationer där hög informationssäkerhet och tillgänglighet är av stor vikt, så som banksektorn. I dagens samhälle spelar Internet en central roll, och risken att en samhällskritisk tjänst skulle otillgängliggöras anses överhängande. Arbete krävs således inom området för att säkra den data-infrastruktur som Internet utgör.

Begreppet effektivitet används här som ett sammansatt kvalitetsvärde i vilket hänsyn tas inte endast till verkningsgrad, det vill säga hur väl attacker kan upptäckas, motverkas eller lindras, utan också till faktorer vilka spelar in i beslut kring huruvida lösningen är en ekonomiskt motiveringsbar åtgärd för att skydda tjänster. Dessa faktorer innefattar resursåtgång såväl vid normaltillstånd som under en attack. Det är av yttersta vikt att den mekanism som används för att skydda mot DoS-attacker i sig inte märkbart försämrar tillgängligheten vid normaltillstånd. Än mer problematiskt blir detta i miljöer där hög tillgänglighet är mindre kritiskt än den genomsnittliga tiden det tar för en klient att ansluta en tjänst.

3.1 Delproblem

För att förenkla en metodisk lösning av problemet bryts detta ner i flera mindre delproblem. Dessa delproblem löses därefter i sekvens. Vid genomförande av de senare delmålen används resultat från tidigare delmål för att besvara dessa frågeställningar.

De delproblem som anses relevanta för att lösa det aktuella problemet definieras som följer:

1. Efter uppdelningar av olika tillvägagångssätt som används för att upptäcka, motverka och lindra effekterna av SYN flood-attacker, vilka lösningar finns i dagsläget på problemet samt vilka av dessa behöver väljas ut för att ge underlag för en representativ undersökning av befintliga skyddsmetoder? När detta delmål är genomfört bör en representativ samling skyddsmetoder finnas.
2. Vilka styrkor respektive svagheter kan identifieras hos de lösningar som undersöks? Kan dessa antas representativa för den kategori lösningen tillhör? För att svara på dessa frågor behöver en genomgång göras av hur de utvalda skyddsmetoderna fungerar. Då dessa frågor besvarats bör en lista över egenskaper för samtliga av de utvalda skyddsmetoderna sammanställts.
3. Vilka system kan förväntas komplettera varandra i det fall de skulle kombineras? För att kunna avgöra hur väl skyddsmetoder kan kombineras bör effektivitet så som det är definierat ovan användas som mått. Efter dessa frågor besvarats bör en lista finnas över de kombinationer av skyddsmetoder som kan antas innebära ökad effektivitet samt motivering för detta. Utfallet från genomförandet av detta delmål bör utgöras av en lista av möjliga kombinationer av skyddsmetoder samt fördelar och nackdelar med dessa.
4. Vilken form av skydd är bäst motiverad för olika typer av organisationer, beroende på deras respektive krav på tillgänglighet? Inte alla organisationer har ett befogat behov av den lösning med högst verkningsgrad. I somliga fall kan hotbilden och den negativa påverkan förväntas vara liten nog att SYN flooding inte utgör en stor nog risk för att motivera att ett avancerat skydd implementeras. Dessutom kan det förväntas finnas olika lösningar som är mer effektiva givet specifika scenarion. Den slutgiltiga produkten av detta arbete förväntas vara en rekommendation för hur organisationer med TCP-baserade tjänster kan skydda dessa mot DoS-attacker som utnyttjar SYN flooding. Behovet av en sådan metod speglas såväl i den statistik från Hansson (2010) som presenterats i kapitel 1, samt enligt Internet Engineering Task Force (2007).

3.2 Avgränsningar

En undersökning av samtligt material producerat inom området vore alltför omfattande för detta arbete, och därför undersöks en samling skyddsmetoder vilka begagnar skilda tillvägagångssätt för att motverka SYN flooding-attacker. Det är dessutom troligt att ytterligare skyddsmetoder finns vilka hade varit relevanta för undersökning. En vidare undersökning av denna sak kan således vara motiverad i framtida arbeten inom området.

4 Metod

Nedan följer en redogörelse för hur genomförandet av detta arbete bör fortskrida för att nå uppsatta mål och delmål. Följer gör också en motivering för varför denna metod valts, samt möjliga alternativa ansatser för att lösa det problem som definierats i kapitel 3.

En mer detaljerad genomgång följer här av hur arbetet kommer genomföras uppdelat efter de delmål som presenterats i kapitel 3.

1. Arbetet med att hitta de skyddsmetoder som kommer undersökas i denna rapport startar i klassificeringar av typer av skyddsmetoder indelade efter hur metoderna i fråga angriper problemet att upptäcka, motverka och lindra effekterna av SYN flooding-attacker. Utifrån sådana klassificeringar kan metoder väljas i ett försök att nå ett representativt urval. De skyddsmetoder som inte testas är således förhoppningsvis ej alltför olika de som väljs ut under genomförande av detta steg. En klassificering presenteras av Internet Engineering Task Force (2007), från vilken en sökning efter relevanta artiklar kan utgå. Skulle denna klassificering ej anses tillräcklig kan vidare, med motivering, ytterligare skyddsmetoder väljas ut för vidare analys. Det material som ligger till grund för senare analys av skyddsmetoder bör komma från väl accepterade källor, så som kollegialt utvärderade artiklar eller standarder presenterade som Internet Engineering Task Force Request For Comments. En alternativ ansats hade varit att kontakta framstående företag inom området för dokumentation av de metoder som dessa använder för att bekämpa SYN floods. Det antas dock att få företag skulle vara villiga att lämna ut en sådan djupgående beskrivning av de program som de marknadsför och säljer, då ett arbete som detta inte lagligen kan sekretessbeläggas. Utöver detta problem kan andra tänkas finnas så som brist på sådan dokumentation eller andra faktorer vilka medför att företag inte skulle vara intresserade av att dela med sig av sitt kunnande. Valet för vilken typ av litteratur som väljs motiveras också av antagandet att de skyddsmetoder som finns presenterade i den väl accepterade litteraturen som nämnts ovan ligger till grund för de kommersiella skydd som finns på marknaden idag. Det förväntade resultatet från genomförandet av delmål 1 är en samling skyddsmetoder som kan användas för genomförande av delmål 2.
2. Skyddsmetoderna bör undersökas genom en analys av deras respektive beskrivningar, då en praktisk testning av samtliga vore alltför omfattande för det aktuella arbetet. Denna analys blir således en litteraturanalys av de olika artiklarna i vilka skyddsmetoderna i fråga är presenterade. Utifrån hur de beskrivs i dessa artiklar bör resonemang föras kring deras funktion för att utvärdera förväntad effektivitet. Hänsyn bör således tas till faktorer som förbrukning av systemresurser i form av nätverksbandbredd, ökad fördröjning för legitim nätverkstrafik, minnesintensitet samt förväntat utnyttjande av processortid utöver förmågan att upptäcka, motverka och lindra effekterna av en SYN flood-attack. En exakt bedömning kan inte förväntas, men genom solitt resonemang bör för varje skyddsmetod kunna listas styrkor och svagheter i ovan nämnda aspekter. Resonemang bör också föras kring huruvida de analyserade skyddsmetoderna är representativa i sin funktionalitet för den kategori de tillhör, och i så fall också om de upptäckta vinsterna eller bristerna hos aktuell skyddsmetod kan antas gälla för samtliga metoder av denna kategori. Dessa listor agerar sedan underlag för genomförande av delmål 3.

3. Genom vidare analys av resultatet från genomförande av delmål 2 bör undersökas om utvalda skyddsmetoder kan antas komplettera varandra i det fall de skulle kombineras. Målet vid genomförandet av detta delmål är att kunna finna sammanhang sådana att skyddsmetod A är ineffektiv i avseende X, men effektiv i avseende Y medan skyddsmetod B är ineffektiv i avseende Y, men effektiv i avseende X. En kombination av de båda bör då utvärderas för att undersöka om denna skulle medföra att samtliga fördelar kan utnyttjas medan de negativa aspekterna med respektive skyddsmetod kan minskas eller utplånas. Resonemang bör föras kring såväl de kombinationer som antas öka effektiviteten, som de där effektiviteten kan förväntas vara minskad. Med hjälp av de listade fördelar och nackdelar som funnits under genomförande av delmål 2 bör en lista skapas vilken innehåller kombinationer av skyddsmetoder samt en utvärdering av deras förväntade kompatibilitet.
4. För att avgöra vilka skyddsmetoder som bör implementeras av organisationer för att bekämpa SYN flooding-attacker måste resonemang föras kring resultaten av tidigare delmål. Från detta resonemang bör en metodisk lista över rekommendationer kunna skapas. Dessa rekommendationer bör vara anpassade för att passa såväl mindre utsatta som mer utsatta organisationer. Det slutgiltiga resultatet av genomförande av detta delmål bör styrka den ursprungliga tesen.

Problem som kan uppstå under arbetet är brist på information kring en eller flera skyddsmetoder eller brist på beskrivna skyddsmetoder inom en viss kategori. Skulle information vara knapphändig kan vissa antaganden göras, om dessa möjliggör en analys. Samtliga antaganden som görs måste tydligt presenteras som sådana, och resonemang baserade på antaganden bör redovisas som mindre tillförlitliga. Skulle en svagt dokumenterad metod tyckas mycket lovande ur effektivitetssynpunkt bör detta anges även i slutsatserna. Resonemang kan också föras kring huruvida skyddsmetoder tillhörande en kategori för vilken exempel saknas skulle kunna kombineras med andra.

Skulle kombinationer av skyddsmetoder över lag tyckas negativt påverka effektiviteten falsifierar detta således den tes efter vilket arbetet utförts, om inte helt så delvis. I detta fall bör då utvärderas individuella skyddsmetoder samt motiveras hur dessa är mer effektiva än kombinationer av flera sådana. Rekommendationer bör fortfarande kunna ges för hur enskilda skyddsmetoder bör implementeras för att effektivt skydda utsatta tjänster.

5 Lokalisera relevanta skyddsmetoder

Följande kapitel syftar till att besvara delmål 1 presenterat i kapitel 3 genom att undersöka existerande skyddsmetoder för att lokalisera sådana som är relevanta för fortsatt arbete.

5.1 Skyddsmetoder enligt Request For Comments 4987

Enligt Internet Engineering Task Force (2007) finns flera olika vägar att angripa problemet. De skyddsmetoder som vidare kommer undersökas i detta kapitel väljs för att representera denna indelning.

5.1.1 Filtrering

Den första metoden som tas upp av Internet Engineering Task Force (2007) är filtrering. Filtrering utfört vid routers i nätet kan försvåra IP spoofing och därigenom omöjliggöra många SYN flooding-attacker, då dessa är i stort beroende av möjligheten att kunna spoofa adresser. IP spoofing är ett problem som är relevant i fler avseenden än bara problemet med SYN flooding, och någon djupgående analys av hur IP spoofing kan motverkas ligger utanför omfattningen av detta arbete. *Network Ingress Filtering* kommer dock behandlas som en skyddsmetod i vidare undersökning. Som underlag för detta används Internet Engineering Task Force, (2000a).

5.1.2 Inställningar för TCP-implementationer

Internet Engineering Task Force (2007) diskuterar förändringar av inställningar i TCP-protokollet. Mer specifikt tas upp är en ökad storlek för backlog alternativt en sänkt time-out för halvöppna sessioner. Dessa metoder avfärdas dock som otillräckliga eller problematiska. En större backlog innebär enligt Lemon (2002) problem då TCP-implementationer inte designats för att kunna hantera backlogs större än några hundra halvöppna sessioner åt gången. Ett problem som pekas ut av Internet Engineering Task Force (2007) angående sänkt time-out för halvöppna sessioner är att en andel legitim trafik, härstammande från förbindelser med hög fördröjning, kan stängas ute. Dessutom pekas det ut att för att genomföra en lyckad attack mot en maskin som använder sänkt time-out krävs endast en linjärt växande mängd SYN-segmet. Detta kan antas vara sant även för större backlog. På grund av dessa uppenbara problem, vilka redan dokumenterats, kommer ej vidare analys ske av denna typ av skydd mot SYN flooding-attacker.

Nästkommande metod som tas upp av Internet Engineering Task Force (2007) är att återanvända den äldsta halvöppna sessionen vid nya inkommande SYN-segment. Problemet som pekas ut med denna ansats till att lösa problemet är att om legitim trafik inte kan etablera en förbindelse innan backlogen återigen fyllts upp kommer sådan trafik stängas ute. Detta är ett problem framförallt vid en stor mängd inkommande SYN-segment, så som vid en kraftfull attack eller en om backlogens storlek är för liten. Som nämnt ovan är det dock problematiskt att öka storleken på backlogen. Då uppenbara problem redan pekats ut med denna metod kommer den inte undersökas vidare. Det bör dock ämnas att det sannolikt är mer effektivt att återanvända halvöppna sessioner kombinerat med en något utökad backlog samt sänkt time-out för halvöppna sessioner än att inte tillämpa något skydd alls.

5.1.3 SYN cache

Vidare tar Internet Engineering Task Force (2007) upp SYN cache som presenteras av Lemon (2002). Denna artikel är refererad av Internet Engineering Task Force (2007) och kommer utgöra grunden för undersökning av SYN cache.

5.1.4 SYN cookies

Lemon (2002) behandlar också, till viss del, konceptet SYN cookies, vilket också tas upp av Internet Engineering Task Force (2007). Båda de ovan nämnda texterna används som underlag för vidare analys av SYN cookies.

5.1.5 Brandväggsbaserade skyddsmetoder

Den sista kategori som nämns av Internet Engineering Task Force (2007) är brandväggsbaserade lösningar. En brandväggslösning presenteras av Schuba et al., (1997). Denna kommer undersökas vidare som representant för brandväggsbaserade lösningar. Motivation för detta är enkelheten i funktionen hos denna lösning. Flera andra brandväggsbaserade lösningar finns, exempelvis talar Safa et al. (2007) om Firewall-1 (Gonclaves & Brown, 1999). Målet med arbetet bakom denna rapport är dock att snarare att finna trender för vilka typer av skydd som kan kombineras, snarare än att lokalisera individuella lösningar. Skulle en annan brandväggsbaserad lösning än den presenterad av Schuba et al. (1997) finnas bör denna kunna användas i stället i de kombinationer av skyddsmetoder i vilken brandväggsbaserade lösningar över lag kan antas vara fördelaktiga.

5.2 Kompletterande skyddsmetoder

Samtliga metoder presenterade av Internet Engineering Task Force (2007), med undantag för filtrering, är baserade på att hantera problemet med SYN flooding på maskinnivå. Andra skyddsmetoder, vilka arbetar på en nätverksnivå har också presenterats. Beteendet hos sådana skyddsmetoder varierar till den grad att det anses fördelaktigt att analysera mer än en. De metoder som väljs ut bör således inte vara inbördes lika i hur de arbetar. De nätverksbaserade lösningar som kommer analyseras närmare är de presenterade av Wang et al. (2002a) fortsatt i Wang et al. (2002b), Ohsita et al. (2005) respektive Safa et al. (2007). Dessa tre skyddsmetoder arbetar på olika sätt, med gemensamt att problemet med SYN flooding angrips på nätverksnivå.

Wang et al. (2002a) samt Wang et al. (2002b) syftar endast till att upptäcka attacker utförda från det nätverk i vilket lösningen implementerats.

Safa et al. (2007) försöker lindra påverkan från attacker genom att placera skyddsmetoden i det nätverk den spoofade avsändaradressen tillhör.

Ohsita et al. (2005) presenterar en skyddsmetod som hindrar trafiken från angripare att nå offret efter att en attack har upptäckts.

Metoderna väljs då de arbetar på tre olika platser i nätverket; angriparens nätverk (Wang et al., 2002a; Wang et al., 2002b), offrets nätverk (Ohsita et al. 2005) respektive det spoofade nätverket (Safa et al., 2007). Dessa metoder är ett urval av nätverksbaserade ansatser till att lösa problemet SYN flooding utgör. En mängd ytterligare skyddsmetoder finns definierade vilka arbetar på en nätverksnivå. Dessa tre har valts ut då de anses förhållandevis gemensamt representativa för nätverksbaserade skyddsmetoder i stort då de representerar samtliga möjliga implementationsplatser samt tre vitt skilda sätt att angripa problemet

5.3 Sammanfattande listning av utvalda skyddsmetoder

Sju skyddsmetoder har valts ut för vidare analys. Dessa är:

- *Network Ingress Filtering*, eller filtrering.
- SYN cookies.
- SYN cache.
- De brandväggsbaserade skyddsmetod som presenterats av Scuba et al. (1997), vidare brandväggsbaserad lösning.
- Den nätverksbaserade skyddsmetod presenterad av Wang et al. (2002a) fortsatt i Wang et al. (2002b), vidare Nätverksbaserad lösning A.
- Den nätverksbaserade skyddsmetod presenterad av Ohsita et al. (2005), vidare Nätverksbaserad lösning B.
- Den nätverksbaserade skyddsmetod presenterad av Safa et al. (2007), vidare Nätverksbaserad lösning C.

Denna förteckning anses lösa delproblem 1, presenterat i kapitel 3.

6 Beskrivning och analys av utvalda skyddsmetoder

Nedan följer en beskrivning av samtliga skyddsmetoder som valdes ut i kapitel 5. Utöver en beskrivning av funktionaliteten av den aktuella skyddsmetoden beskrivs dessutom den kategori av skyddsmetoder denna tillhör. Funktionaliteten analyseras för att skapa en nöjaktig beskrivning av styrkor respektive svagheter hos den aktuella metoden samt tillhörande kategori.

6.1 Filtrering

Då SYN flooding är beroende av IP spoofing som nämnts tidigare, kan attacker omöjliggöras eller försvåras om angriparens möjligheter att spoofa avsändaradresser begränsas. En metod för att stoppa IP spoofing kallad *Network Ingress Filtering* är presenterad av Internet Engineering Task Force (2000a). Funktionaliteten är tämligen enkel i sin principiella form och implementeras av internetleverantörer på routrar närmast kunden alternativt av företag på routern närmast det publika Internet. Det vill säga en så kallad edge router. Den filtrerande routern tillåter endast paket skickade från det lokala nätverket om avsändaradressen tillhör detta nätverk. Alla försök att spoofa avsändaradresser till någon adress utanför det lokala nätverket kommer således innebära att trafiken stoppas innan den hinner nå Internet.

6.1.1 Förväntade styrkor och svagheter

Eftersom IP spoofing idag fortfarande är ett problem, trots att *Network Ingress Filtering* presenterades för nära ett decennium sedan kan antas att lösningen inte är slutgiltig. Det främsta problemet tycks vara täckningsgraden som krävs för att effektivt hindra IP spoofing. En sofistikerad angripare kommer inte välja en internetleverantör som tillämpar filtrering om alternativ finns som inte filtrerar. Allt som krävs för att en IP spoofing-baserad attack som SYN flooding ska kunna genomföras är att just den router till vilken angriparen är inkopplad inte tillämpar filtrering. Kostsamma övergångar till nyare teknik, där vinsten blir signifikant först när en överväldigande majoritet genomfört övergången är ofta trögstartade. Ett exempel på detta är övergången från IP version 4 till version 6. Eftersom Internet spänner över nationsgränser kan lagkrav på filtrering hos internetleverantörer inte heller förväntas realiseras i samtliga länder där internetaccess finns tillgängligt. Dock innebär varje router där *Network Ingress Filtering* implementeras att ännu några ytterligare potentiella angripare hindras från möjligheten att enkelt genomföra attacker. Det kan med någorlunda säkerhet antas att en markant del av mindre SYN flooding-attacker utgår från angripare vilka inte är engagerade nog för att undersöka huruvida filtrering finns implementerad på den närmsta edge routern och om så är fallet byta internetleverantör, alternativt från zombier i så kallade botnets. En angripare kan inte kontrollera vilken internetleverantör de faktiska ägarna av zombie-maskinerna väljer.

Ett mer tekniskt problem med filtrering är det ökande behovet för mobila tjänster. Mobila noder som behåller sin IP-adress, enligt Internet Engineering Task Force (2002), oavsett vilket nätverk de använder för att nå Internet, kommer blockeras av ovan beskrivna filter. Trafik till noden skickas i dessa fall genom en tunnel, medan trafik från noden inte är "tunnlad". En beskrivning för *reverse tunneling* är gjord av Internet Engineering Task Force (1998). En genomgång av mobilt IP faller utanför omfattningen av detta arbete och kommer inte vidare behandlas.

Network Ingress Filtering begränsar effektivt möjligheten att spoofa avsändaradresser utanför den tillåtna adressrymden. Attacker kan dock fortfarande genomföras genom spoofande av adresser inom denna rymd.

6.2 SYN cookies

Effektiviteten i en SYN flooding-attack härstammar från beteendet hos TCP som innebär att resurser allokeras hos en mottagare av ett SYN-segmet redan innan en session är helt etablerad. SYN cookies är ett försök att lösa problemet genom att ändra detta faktum. Lösningen implementeras på potentiella offer för SYN flooding-attacker.

En SYN cookie är ett särskilt valt sekvensnummer i vilket information om noden som initierat kommunikationen inkluderats genom serverns hemliga funktion. Då servern mottar ett SYN-segment genererar den ett sekvensnummer som innehåller en tidsstämpel från serverns specifika timer för ändamålet samt en hash. Denna hash skapas av en kombination av olika värden som servern sedan kan använda för att verifiera svar. Intressanta sådana värden är tidstämpel, det sekvensnummer som använts för SYN-segmentet, MSS (Maximum Segment Size), avsändaradress och avsändarport. Olika implementationer finns vilka varierar i hur data kodas in i sekvensnumret. Den metod som beskrivs av Internet Engineering Task Force (2007) använder en timer på 32 bitar. Denna timer modulo 256 ockuperar de första 5 bitarna i SYN cookien. Dessa 5 bitar följs av tre bitar för MSS samt 24 bitar för en hash av avsändar- och mottagaradresser samt avsändar- och mottagarportar.

Ett SYN/ACK-segment skickas sedan från servern med sekvensnumret satt till den genererade SYN cookien. Ingen tillståndsförändring sker och inga resurser allokeras. Vid normalt beteende tar klienten som initierade sessionen emot detta SYN/ACK-segment varpå denna svarar med ett ACK-segment med ACK motsvarande SYN cookien ökad med ett. När servern mottar ett ACK-segment för en session som inte är öppen så undersöker den om den motsvarar en SYN cookie som kan ha genererats från något av de senaste klock-värdena samt de värden som kan utvinnas ur det mottagna paketet, det vill säga adress- och portvärden. All information kring sessionen finns alltså tillgänglig i ACK-segmentet och inga resurser har behövts utnyttjas hos servern för att spara dessa. Skulle avsändaradressen för SYN-segmentet vara spoofad finns ingen halvöppen session, och servern väntar inte på svar (Internet Engineering Task Force, 2007).

6.2.1 Förväntade styrkor och svagheter

SYN cookies kringgår behovet för en backlog och förhindrar därmed att SYN flooding-attacker kan genomföras alls. Dock introduceras nya problem, det främsta av vilka är att SYN-segment innehåller vissa inställningsflaggor för funktionalitet som den anslutande parten vill utnyttja under sessionen. Sekvensnummerfältet i vilken SYN cookien placeras är för kort för att information om dessa val ska kunna kodas in i SYN cookien. Detta innebär att viss funktionalitet i TCP omöjliggörs av användandet av SYN cookies. Mest signifikant är förlusten av möjligheten att modifiera storleken på fönstret, så kallad *window scaling* (Internet Engineering Task Force, 2007; Lemon, 2002).

6.3 SYN cache

Som nämnts i kapitel 5 är datastrukturen för backlogen inte skalbar. En lång lista av poster blir problematisk exempelvis då slumpvisa poster behöver kastas på grund av överbelastning då ett system utsätts för en SYN flooding-attack. Eftersom en lista måste gås igenom sekventiellt för att nå det element som behöver kastas krävs att i genomsnitt halva längden av listan måste passeras varje gång. Då längden av denna lista ökas ökar således också tiden som krävs för att kasta en post i listan och därigenom öppna plats åt nya inkommande förbindelseförfrågningar. Detta innebär således att en ökad storlek på det attackerade systemets backlog kan öka de negativa konsekvenserna av en SYN flooding-attack (Lemon, 2002).

SYN cache innebär att utformningen av backlogen helt byts ut mot en global hashtabell. Varje inkommande SYN-segment skapar en ny "hink" i denna hashtabell där data lagras för anslutningen. Den maximala storleken på den globala tabellen samt på individuella hinkar kan sättas för att säkerställa en maximal minnesförbrukning samt maximal processortid som krävs för att söka igenom tabellen (Lemon, 2002).

6.3.1 Förväntade styrkor och svagheter

Liksom med den tidigare lösningen för backlogen innebär storleksbegränsningen att en total uttömning av serverns resurser inte kan ske genom en DoS-attack. SYN cachen kan dock överfyllas vid en SYN flood (Lemon, 2002).

Möjligheten att attackera en specifik hink och överfylla denna med resultatet att en maskin aldrig skulle kunna etablera en session är mycket liten. Detta på grund av att index för hinkar i hashtabellen beräknas utifrån avsändar- och mottagaradresser, avsändar- och mottagarportar samt ett hemligt värde. För att nå den hink som angriparen försöker överfylla måste denna således gissa portnummer samt det hemliga värdet. Skulle en hink överfyllas och den legitima trafiken hindras kommer detta behöva upprepas för en ny hink om den anslutande maskinen gör ett nytt försök med ny avsändarport samt ny hemlighet (Lemon, 2002). Riktade angrepp för att förhindra specifika maskiner från att nå den attackerade tjänsten, blir således närmast omöjliga. Skulle en SYN cache implementeras utan att bruka hemligheter för samtliga hinkar hade riktade attacker av denna typ kunnat vara problematiska.

Övergripande gäller att en SYN cache lider av stort sett samma problem som en vanlig backlog, dock i lägre utsträckning. Vid en kraftig SYN flooding-attack kommer hashtabellen överfyllas med nya hinkar vilket innebär att slumpvisa hinkar kastas och därmed kan legitim trafik förhindras. I testning genomförd av Lemon (2002) kan under en SYN flood av 15 000 paket per sekund i princip samtliga legitima sessioner startas inom en sekund. Under en betydligt kraftfullare attack kan dock antas att resultatet skulle försämras.

SYN cache implementeras genom att TCP/IP-beteendet hos operativsystemets kärna modifieras. Detta kan vara en stötesten vid implementering då lösningen inte kan bifogas i programvara som distribueras. Beroende på vilket operativsystem som används på den maskin som erbjuder tjänsten som skall skyddas kan svårighet i implementation av ytterligare funktionalitet i kärnan variera. För *open source*-system bör, om koden för sådan implementation finns tillgänglig, en förhållandevis enkel omkompilering av kärnan kunna göras, alternativt en modul läggas till. För stängda operativsystem kan implementation av en sådan förändring till kärnan vara betydligt mer problematisk, i det fallet utvecklaren av operativsystemet är ovillig att implementera skyddsmetoden.

SYN cache anses vara en lovande metod då den enligt Lemon (2002) ökar effektiviteten inte bara under attack utan även vid normal trafik då mindre minne krävs samt halvöppna sessioner är enklare att extrahera från backlogen. SYN cache tycks endast bringa fördelar, vilka bör anses motivera det eventuella arbete som krävs för att implementera skyddsmetoden. Skulle däremot SYN cache användas i kombination med en brandväggsbaserad skyddsmetod, som till någon grad fungerar som relay som definierat av Schuba et al. (1997), kan eventuellt det skydd vid en attack som erbjuds av SYN cache att vara redundant. En implementation av SYN cache kan dock ändå vara motiverad om sessionsetablering för TCP konsumerar en märkbar andel systemresurser.

6.4 Brandväggsbaserad lösning

Det karaktäristiska draget för en brandväggsbaserad lösning är att den inför en mellanliggande part, det vill säga en brandvägg, som hanterar trafik i offrets ställe. Den mellanliggande parten kan analysera trafik samt modifiera vissa aspekter av trafiken eller injicera egna skräddarsydda paket för att mildra konsekvenserna av en SYN flooding-attack. En brandväggsbaserad lösning kan rent tekniskt placeras på flera platser, exempelvis på den utsatta maskinen, på en separat maskin eller på en router genom vilken trafiken flyter. En brandvägg kan, om den är placerad på ett strategiskt riktigt ställe, skydda flera tjänster. Detta innebär bland annat att endast en central punkt måste uppdateras för att implementera skyddet.

Innan presentationen av den utvecklade lösningen talar Schuba et al. (1997) om aspekter de anser viktiga hos en lösning. Dessa lyder som följer:

- Oberoende av operativsystem och implementation av TCP/IP-stack hos de skyddade systemen.
- Inga krav på förändring av IP- eller TCP-protokollen.
- Möjlighet att skydda grupper av system.
- Inga särskilda hårdvarukrav.
- Portabilitet.
- Skalbarhet.
- Möjlig att konfigurera.

Samtliga dessa krav kan sägas uppfyllas av en brandväggsbaserad lösning. Vidare diskuterar Schuba et al. (1997) två huvudsakliga tankesätt för brandväggsbaserade lösningar; relay samt semitransparent gateway. En lösning av typen relay tar över uppsättandet av en ny session i dess helhet, och efter att denna etablerats sätts en ny session upp mellan brandväggen och den skyddade tjänsten. Därefter måste brandväggen för varje paket översätta sekvensnummer för att data ska kunna flyta mellan de två ändparterna. Problemet som pekas ut med denna lösning är framförallt den tid det tar för brandväggen att översätta sekvensnummer samt risken att brandväggen kollapsar under trycket av en SYN flooding-attack. En semitransparent proxy låter istället SYN-segmentet passera till den skyddade maskinen, samt lyssnar efter utgående SYN/ACK-segment. När ett sådant passerar svarar brandväggen med en matchande ACK varefter en av två scenarion kommer inträffa. Om avsändaradressen är legitim kommer även denna skicka ett ACK-segment. TCP kan dock hantera dubbla meddelanden och kastar det nyinkomna ACK-segmentet utan att detta påverkar sessionen. Om avsändaradressen är spoofad kommer brandväggen efter en bestämd tid att generera och skicka ett RST-segment vilket avslutar sessionen. Det huvudsakliga syftet med en sådan lösning är att så fort som möjligt flytta en session från ett halvöppet till ett öppet tillstånd. I ett öppet tillstånd finns fortfarande resursbehov, dock betydligt mindre. (Schuba et al., 1997.)

Lösningen som föreslås av Schuba et al. (1997) arbetar tämligen likt en semitransparent gateway. Den grundläggande lösningen är dock utökad med en mekanism för klassificering av avsändaradresser. Fem olika kategorier finns:

1. *Good*: adresser från vilka normal TCP-trafik observerats.
1. *Bad*: adresser från vilka SYN observerats men ingen vidare trafik observerats.
2. *New*: adresser som anses suspekta, men ännu inte klassificerats som *good* eller *bad*.
3. *Perfect*: godkända adresser konfigurerade av administratör.
4. *Evil*: icke godkända adresser konfigurerade av administratör.

Samtliga adresser som inte tillhör någon av ovanstående kategorier tillhör automatiskt kategorin *null* för vilken inga speciella regler finns. Anledningen att denna kategori finns är att det är orimligt att föra register över samtliga möjliga adresser. Adresser klassificeras efter vilken trafik brandväggen kan observera genom att lyssna på inkommande trafik. Beroende på vilken avsändaradress som används på inkommande SYN-segment hanterar brandväggen trafiken på olika sätt. För SYN från adresser klassificerade som *good* eller *perfect* ingriper brandväggen inte. För adresser i kategorierna *bad* eller *evil* skickas en RST å SYN-avsändarens vägnar för att avsluta den halvöppna sessionen och frigöra resurser snarast möjligt. Beteendet för behandling av anrop från adresser klassificerade som *new* är likt det för semitransparenta proxies beskrivet ovan. Praktiskt sett betyder detta att om en adress misslyckas med att skicka en ACK för att öppna en session helt klassificeras denna som spoofad och vidare förbindelseförfrågningar från denna avslutas av brandväggen. Om en adress som tidigare ansetts som *bad* skickar en ACK alternativt RST kommer denna klassificeras som *new*. För motsvarande beteende hos adresser klassificerade som *good* finns en förfallotid efter vilken adressen inte längre anses pålitlig. Detta för att förebygga att adresser som tidigare spoofats inte kan skapa legitima förbindelser respektive att adresser som tidigare använts för legitim trafik inte skall kunna användas för att genomföra en attack då dessa inte längre är i bruk (Schuba et al., 1997).

6.4.1 Förväntade styrkor och svagheter

Ett problem med just denna brandväggslösning är att den kan läras upp av en angripare genom att denne spoofar ACK- eller RST-segment för en mängd adresser, vilket innebär att dessa klassificeras som *good*. Angriparen kan sedan använda dessa synbart legitima adresser för att genomföra attacken (Schuba et al., 1997).

Vidare kan problem med denna lösning uppstå vid en kraftfull attack. I detta fall riskerar offrets resurser att uttömmas genom att en ofantlig mängd sessioner öppnas fortare än brandväggen skickar RST-segment. Även vid en mildare attack finns en avsevärd risk för att tjänsten försämras. Sätts tiden inom vilken svar måste fåtts innan ett RST-segment skickas för låg kommer legitima förbindelser med hög fördröjning att omöjliggöras. Denna tid måste således sättas med eftertänksamhet. Risk finns dessutom att brandväggen agerar flaskhals om stora mängder trafik måste processeras.

Ytterligare problematik uppstår om samtliga SYN-segment som skickas har separata spoofade avsändaradresser. I detta fall kommer samtlig attacktrafik klassificieras som *new* snarare än *bad*.

6.5 Nätverksbaserade lösningar

Flera olika nätverksbaserade lösningar undersöks då ingen representativ skyddsmetod kunnat identifieras. De tre undersökta skyddsmetoderna delas upp efter vart i nätverket de verkar.

6.5.1 Nätverksbaserad lösning A

Wang et al. (2002a) presenterar en metod för att upptäcka om en SYN flooding-attack utgår från ett nätverk där denna metod är implementerad. Efter att en attack upptäckts kan dynamiskt en annan skyddsmetod aktiveras vilken hanterar attacken. Resursförbrukningen i normalläge kan därigenom sänkas. Metoden går ut på att jämföra antalet utgående SYN-segment med antalet FIN- eller RST-segment. Vid normal kommunikation bör antalet vara exakt symmetriskt där varje session öppnas och stängs under ordnade former. I verkligheten är detta inte alltid fallet, vilket innebär att en viss tolerans bör finnas för exempelvis segment förlorade på nätverket eller maskiner som kraschar med öppna TCP-sessioner. Denna metod har ingen inbyggd potential att stoppa attacker utan syftet är endast att upptäcka dem. En implementation av denna typ skulle också vid offrets sida kunna upptäcka en inkommande attack i hur antalet inkommande SYN och utgående FIN eller RST är osymmetriskt (Wang et al. 2002a). Det torde dock finnas enklare sätt att upptäcka inkommande SYN flooding-attacker vid offret.

Enligt Wang et al. (2002b) skall utsända SYN-segment motsvaras av ett SYN/ACK-segment då motparten i TCP-sessionen svarar på det initiala SYN-segmentet. Om antalet utgående SYN-segment är avsevärt större än antalet inkommande SYN/ACK-segment är sannolikheten stor att en attack utförs. Denna metod i jämförelse med den tidigare nämnda har dessutom fördelen att TCP-sessionens längd inte behöver tas hänsyn till. Vid jämförande av SYN-segment och FIN- alternativt RST-segment genereras de olika intressanta segmenten vid början respektive slutet av en session, medan vid jämförelse av SYN-segment och SYN/ACK-segment tidsskillnaden är betydligt lägre.

6.5.1.1 Förväntade styrkor och svagheter

Wang et al. (2002a) menar att SYN floods så milda som 50 SYN-segment per sekund upptäcks fort och effektivt. Detta får anses närmast omöjliggöra genomförandet av en oupptäckt attack.

Ett stort problem med metoden är att den helt kan kringgås genom att angriparen spoofar ett symmetriskt antal FIN- eller RST-segment. Detta problemet angrips vidare av Wang et al. (2002b) genom att jämföra utgående SYN-segment med inkommande SYN/ACK-segment en *Round Trip Time* (RTT) senare. Inkommande SYN/ACK-segment kan spoofas av en sofistikerad angripare som kontrollerar en proxy utanför nätverket från vilken attacken genomförs. Det kan dock antagas att en stor andel av alla potentiella angripare inte har den kunskap eller de medel som krävs för att genomföra detta. Den totala mängd trafik som krävs för att genomföra en attack oupptäckt ökar dessutom till den dubbla.

6.5.2 Nätverksbaserad lösning B

En lösning som presenteras av Tupakula et al. (2004) skapar ett överliggande nätverk av routers i ett nätverk genom vilket SYN flooding-trafik flyter mot ett offer. Målet med detta nätverk är att ett offer skall kunna meddela en router att en attack pågår vartefter trafiken automatiskt spåras bakåt och blockeras så tidigt som möjligt.

För att bygga ett överliggande nätverk krävs att så många edge routers, det vill säga routers som är placerade i utkanten av det egna nätverket, som möjligt i en domän samarbetar. För att samordna försvaret finns en kontrollant, vilken sedan identifierar samtliga routers genom att tilldela dessa ett unikt *agent-ID*. När någon tjänst utsätts för en attack meddelar denne kontrollanten, som i sin tur omber samtliga agenter att markera all trafik till offret med sitt unika *agent-ID* samt ID för den kontrollant som initierat märkningsprocessen. Om en agent mottager ett paket som redan är markerat med ett *agent-ID* samt ID för kontrollanten i domänen skickas meddelandet vidare utan att märkas. Detta innebär att samtlig trafik som når offret är markerat med det unika *agent-ID* som motsvarar trafikens ingångspunkt i nätverket. Offret kan då kontrollera vilket *agent-ID* SYN flooding-attacken tycks härstamma från. Då detta upptäckts meddelas kontrollanten som därefter instruerar motsvarande agent att kasta attacktrafiken. All trafik från andra agenter kommer fortfarande nå den attackerade tjänsten (Tupakula et al, 2004).

6.5.2.1 Förväntade styrkor och svagheter

Denna metod kan förvisso härleda attacker till en ingångspunkt i offrets nätverk, men då ingen säker differentiering kan göras vid denna ingångspunkt mellan SYN flooding-trafik och legitima TCP-förfrågningar måste samtlig trafik som matchar attacksignaturen stoppas. Detta innebär att stora sektioner av Internet kan nekas tillgång vilket förvisso kan anses bättre än att tjänsten fullkomligt blockeras. Detta faktum gör dock eventuell felsökning mer problematisk. Skulle attacken vara distribuerad över flera olika ingångspunkter i nätverket kan effekten vara närmast identisk med en lyckad attack, eventuellt till och med mer effektiv, om fallet är sådant att trafik blockeras vilken hade kunnat behandlas i det fall attacken var liten nog att hanteras av offret.

Tupakula et al. (2004) lägger stor vikt på möjligheten att skapa mycket smala attacksignaturer vilka kan utvärderas vid ingångspunkten i nätverket. Skulle signaturer kunna skapas vilka kan skilja väl på SYN flooding-trafik och legitim trafik kan denna metod vara intressant för internetleverantörer alternativt stora organisationer. Någon genomgång av hur detta skulle ske, eller hur resurskrävande dessa skulle vara att utvärdera på routers saknas dock.

6.5.3 Nätverksbaserad lösning C

En halvöppen session behålls då inget svar erhålls från den spoofade avsändaradressen för det mottagna SYN segmentet. Om en adress spoofats vilken används av någon maskin kommer denna att generera ett RST-segment som svar på det icke förväntade SYN/ACK-segment som mottags. Safa et al. (2007) föreslår en skyddsmekanism vilken implementeras på edge routers för det nätverk de spoofade adresserna som används för attacken tillhör, för att ovan nämnt beteende skall gälla även för adresser som inte används.

Då den lokala routern i nätverket SYN/ACK-segmentet är adresserat till mottar detta broadcastar den en Address Resolution Protocol (ARP)-förfrågan för att kontrollera att maskinen SYN/ACK-segmentet är adresserat till är online. I normalfallet om inget svar erhålls, exempelvis för att SYN/ACK-segmentet är en produkt av en SYN flooding-attack, kastas SYN/ACK-segmentet och inget vidare sker. Metoden presenterad av Safa et al. (2007) syftar till att ändra detta beteende så att om routern ser en inkommande SYN/ACK adresserad till en oanvänd adress eller icke svarande maskin genereras och skickas ett RST-segment för att återställa sessionen hos SYN/ACK-avsändaren, det vill säga det potentiella offret för en SYN flooding-attack. Detta innebär att om en SYN flood utförs där nätverket som skyddas av denna metod används som källa för spoofade adresser kommer samtliga halvöppna sessioner stängas inom en RTT från offer till det spoofade nätverkets lokala router.

Ett ytterliga problem som löses med denna metod är att skydd byggs in för den sekundära DoS-attack som kan följa av en kraftfull SYN-flood i form av en stor mängd ARP-förfrågningar på nät som utnyttjas för spoofade adresser. Detta genom att tabell upprättas över utgående SYN-segment från nätverket vartefter samtliga inkommande SYN/ACK-segment vilka inte matchar någon SYN i registret kastas, samt besvaras med ett RST-segment. Beteendet blir således som följer: utgående SYN-segment registreras av routern samt en post skapas i en tabell vilken innehåller mottagar- och avsändaradress samt en tidsstämpel. När SYN/ACK-segment adresserade till nätverket tas emot kontrolleras i tabellen huruvida dessa matchar utgående förfrågningar. Om en match finns skickas en ARP-förfrågan för att kontrollera att maskinen är nåbar och responsiv. Fås ett svar på denna skickas SYN/ack-segmentet vidare. Om inget ARP-svar fås skickas ett RST-segment till avsändaren av SYN/ACK-segmentet. Detsamma gäller om det inkommande SYN/ACK-segmentet inte matchar något utgående SYN-segment i tabellen (Safa et al, 2007).

6.5.3.1 Förväntade styrkor och svagheter

Problematiskt med lösningen är att beroende på storlek av tabellen över utgående förfrågningar blir sessionsetablering något långsammare, en svaghet som inte tas upp av Safa et al. (2007). Ett annat enkelt sätt att kringgå denna metod vore att observera resultat av attacker med olika spoofade nätverk för att upptäcka nätverk där metoden föreslagen av Safa et al. är implementerad. Den testning som presenteras av författarna visar att för att nå en högre effektivitet än den brandvägg mot vilken skyddsmetoden jämförs krävs att en stor andel av de nätverk som används för att genomföra en attack har implementerat den föreslagna lösningen. Genomgående högre effektivitet fås först då fler än hälften av dessa nätverk har implementerat skyddsmetoden. Samma problematik gäller alltså som presenterats i kapitel 6.1.1 angående filtrering.

Samtliga mottagna SYN-segment hos offret kommer resultera i halvöppna sessioner vilka kommer ligga kvar i backlogen under en RTT mellan offer och det spoofade nätverket. Vid en kraftfull attack, där hela backlogen kan fyllas under en RTT, skulle detta innebära att attacken inte motverkas över huvud taget. Detsamma gäller om det spoofade nätverket är svårtillgänglig och en RTT är mycket lång.

Det skydd som fås genom en kontroll av ARP-broadcasts i det fall adresser på nätverket där denna skyddsmetod implementeras utnyttjas som avsändaradresser för en SYN flood-attack är dock en mycket positiv bieffekt.

6.6 Sammanfattande listning av styrkor samt svagheter

För att enklare kunna överblicka egenskaper hos ovan beskrivna skyddsmetoder kompletteras dessa med en tabell över förväntad prestation för de olika skyddsmetoderna i vissa avseenden (se Tabell 1). Skalan som används är av kvalitativ typ då en kvantitativ skala i form av sekunder eller byte av minnesförbrukning et cetera skulle kräva genomgående testning av metoderna vilket faller utanför omfattningen för detta arbete. Dessutom väljs få nivåer då någon högre precision inte kan utlovas utan mer ingående testning. Skalan som används har tre nivåer; låg, medel och hög. Låg innebär att en mycket liten avvikelse förväntas jämfört med då skyddsmetoden inte är implementerad. Denna avvikelse bör inte vara märkbar för användare av systemet. Medel motsvarar en märkbar men inte påtaglig förändring. Hög motsvarar en uppenbar förändring i hur systemet påverkas av implementationen av skyddsmetoden.

Egenskaperna som utvärderas i Tabell 1 har valts för att ge en bild av förväntad effektivitet hos respektive skyddsmetoder. Nedan följer en förklaring av varje egenskap samt varför denna är intressant att ta hänsyn till. Tabell 1 avser att lösa delmål 2, presenterat i kapitel 3.

- Implementationsplats. Olika organisationer har olika stor möjlighet att implementera somliga skyddsmetoder. Mindre organisationer, exempelvis, kan inte förväntas kunna kräva implementation av skyddsmetoder utanför det lokala nätverket.
- Svårigheter att implementera. En komplex implementation kan vara dyrbar, och beroende på hur utsatt en tjänst eller organisation är kan det vara mer kostnadseffektivt att välja en annan skyddsmetod.
- Ökad fördröjning för legitim trafik. Tiden som förloras vid attacker måste ställas mot den eventuella extra fördröjning som införs då en skyddsmetod implementeras.
- Resursförbrukning i normalläge. Om resursförbrukningen är för hög vid legitim trafik kan sådan bidra till nedsatt tillgänglighet för tjänsten, så kallad *degradation of service*.
- Resursförbrukning under attack. I det fallet resursförbrukningen stiger okontrollerbart under en attack kan större attacker förväntas medföra en DoS-attack mot skyddsmetoden själv. I de fall denna är implementerad på annan plats än den utsatta maskinen kan detta innebära att ytterligare svagheter införs i nätverket genom implementation av en sådan skyddsmetod.
- Förväntad verkningsgrad vid mindre attacker. Mindre attacker definieras som något en orutinerad hemanvändare med automatiska verktyg, en så kallad *"script kiddie*", skulle kunna genomföra.

- Förväntad verkningsgrad vid kraftfullare attacker. En kraftfull attack definieras som en attack som genomförs av en mer rutinerad angripare med en större mängd resurser, det vill säga möjlighet att skicka långt fler falska SYN-segment. Det antas dock att denna attack inte är kraftfull nog för att skicka nog falsk trafik för att konsumera samtlig nätverksbandbredd hos offret, då detta inte längre främst symboliserar ett SYN flooding-scenario.
- Förväntad verkningsgrad vid distribuerade attacker. Styrkan hos distribuerade attacker tas ej hänsyn till under denna egenskap. Syftet är att undersöka hur de olika skyddsmetoderna hanterar attacker där angreppstrafiken flödar från flera olika platser specifikt. I de fall där ingen särskild extra funktionalitet finns för att motverka distribuerade attacker tilldelas betyget låg.
- Risk att legitim trafik nekas i normalläge. I och med implementation av skyddsmetoder finns en risk att legitim trafik identifieras som attacktrafik och därmed nekas.
- Risk att legitim trafik nekas under attack. Somliga skyddsmetoder tar särskilda åtgärder då en attack upptäckts. Hänsyn tas inte till legitim trafik som nekas på grund av faktorer andra än de tillförda av implementation av skyddsmetoder.
- Representativitet för kategori. Representativitet är intressant för vidare undersökning av kompatibilitet av olika kategorier. Se kapitel 7.

Tabell 1: Sammanfattning av egenskaper hos undersökta skyddsmetoder.

	Förväntad verkningsgrad vid mindre attacker	Resurs-förbrukning under attack	Resurs-förbrukning i normalläge	Ökad fördröjning för legitim trafik	Svårighet att implementera	Implementations-plats
Filtrering	Hög	Låg	Låg	Låg	Hög*	Edge routers
SYN cookies	Hög	Hög***	Hög***	Låg	Medel	Lokal maskin
SYN cache	Hög	Låg	Låg	Låg	Medel	Lokal maskin
Brandväggs-baserad lösning	Hög	Medel**	Medel**	Medel**	Medel	Någon maskin på det lokala nätverket
Nätverksbaserad lösning A	Hög	Låg	Låg	Låg	Låg	Edge routers
Nätverksbaserad lösning B	Hög	Hög	Medel	Låg	Hög	Edge routers
Nätverksbaserad lösning C	Hög	Hög	Medel	Låg	Medel	Edge routers

	Representativitet för kategori	Risk att legitim trafik nekas under attack	Risk att legitim trafik nekas i normalläge	Förväntad verkningsgrad vid distribuerade attacker	Förväntad verkningsgrad vid mer kraftfulla attacker
Filtrering	Hög	Låg	Låg	Medel****	Hög
SYN cookies	Hög	Låg	Låg	Låg	Medel
SYN cache	Hög	Låg	Låg	Låg	Låg
Brandväggs-baserad lösning	Medel	Medel**	Låg*	Låg	Medel
Nätverksbaserad lösning A	Medel	Medel	Låg	Låg	Hög
Nätverksbaserad lösning B	Medel	Hög	Låg	Hög	Hög
Nätverksbaserad lösning C	Medel	Låg	Låg	Låg	Medel

* Implementation av tillräcklig täckningsgrad för att nå hög verkningsgrad

** Förväntas variera beroende på val av implementation.

*** Förlorad prestanda då vissa funktioner hos TCP inte kan utnyttjas jämställs med resursförbrukning.

**** Förväntas variera beroende på täckningsgraden.

7 Analys av kompatibilitet hos undersökta metoder

Generellt kan sägas att om olika skyddsmetoder implementeras på olika platser är det mer troligt att dessa kan kombineras med fördelaktigt resultat. Kompatibilitet varierar dessutom naturligtvis på den specifika funktionaliteten för de skyddsmetoder som önskas kombineras. Värt att notera här är att de tre olika nätverksbaserade skyddsmetoder som undersökts samtliga implementeras på olika platser i nätverket, vilket innebär implementationsplats inte bör ses som ett hinder för att kombinera dessa. Skyddsmetoder som använder vitt skilda angreppsvägar för att motverka SYN flooding-attacker kan också antas generellt vara mer kompatibla.

I kapitel 6.6 presenteras representativitet för kategorier för respektive skyddsmetoder. Kategorierna är de som presenteras i kapitel 5. Denna egenskap är av stort intresse för undersökning av kompatibilitet mellan skyddsmetoder då, om representativiteten anses god, mer generella antaganden kan göras kring kompatibilitet mellan större grupper av skyddsmetoder. Om en kombination av skyddsmetoder förväntas vara effektiv samt samtliga individuella skyddsmetoder anses representativa för den kategori de representerar kan antas att kombinationer av andra skyddsmetoder tillhörande dessa kategorier skulle vara effektiva.

Fall kan existera där olika skyddsmetoder är kompatibla i den meningen att de kan implementeras parallellt men på grund av hur metoderna i fråga hanterar attacker effektiviteten in ökas. Ett exempel på detta är kombinationen presenterad av Lemon (2002) av SYN cookies och SYN cache. Båda dessa metoder är implementerade som förändringar i systemets kärna för att modifiera beteendet hos maskinen i frågas TCP/IP-stack. Vad som praktiskt sker, beroende på funktionaliteten hos dessa skyddsmetoder är att då SYN cachen överfylls börjar SYN cookies användas, vilket helt kringgår SYN cachen. Ingen överlappande funktionalitet finns således i denna kombination av skyddsmetoder, och faktum att effektiviteten för skyddet ökar i avseendet att fler legitima anslutningar kan göras (Lemon, 2002) beror på att SYN cookies är mer effektiva under attacker kraftfulla nog att överfylla SYN cachen. Fall som detta tas ej hänsyn till. För vidare undersökning innebär begreppet kompatibilitet hos skyddsmetoder att dessa kompletterar varandra då de arbetar parallellt.

Tabell 2 sammanställer förväntad vinst av effektivitet vid kombination av de olika skyddsmetoder som undersökts i kapitel 6 och avser således att lösa delmål 3 presenterat i kapitel 3. Skalan Låg – Medel – Hög används liksom tidigare, och anger den förväntade vinsten vid kombination av olika skyddsmetoder. Låg innebär att skyddsmetoderna kan implementeras parallellt, men vinsten är minimal alternativt icke existerande. Medel betyder att en viss vinst av effektivitet bör finnas, samt Hög att inget hinder bör finnas för att med gott resultat kombinera skyddsmetoderna.

I Tabell 2 antas att samtliga skyddsmetoder är implementerade så att de skyddar ett teoretiskt offer. Det är således effektiviteten i motverkande av attacken mot detta teoretiska offer som utvärderas.

Tabell 2: Sammanställning av kompatibilitet hos undersökta skyddsmetoder.

	Filtrering	SYN cookies	SYN cache	Brandväggs-baserad lösning	Nätverks-baserad lösning A	Nätverks-baserad lösning B	Nätverks-baserad lösning C
Filtrering		Hög	Hög	Hög	Hög	Hög	Hög
SYN cookies	Hög		Låg	Låg	Hög	Låg	Låg
SYN cache	Hög	Låg		Hög	Hög	Hög	Hög
Brandväggs-baserad lösning	Hög	Låg	Hög			Medel	Medel
Nätverks-baserad lösning A	Hög	Hög	Hög	Hög		Hög	Hög
Nätverks-baserad lösning B	Hög	Låg	Hög	Medel	Hög		Låg
Nätverks-baserad lösning C	Hög	Låg	Hög	Medel	Hög	Låg	

Mest framträdande från Tabell 2 är mängden kombinationer av skyddsmetoder klassade som "Hög". Detta stärker tesen *"genom att undersöka existerande skyddsmetoder kan rekommendationer ges till organisationer i riskzonen för hur dessa kan utnyttja och kombinera befintliga skyddsmetoder för att effektivare upptäcka, motverka och lindra effekterna av SYN flooding-attacker",* vilken ligger till grund för detta arbete.

Somliga skyddsmetoder tycks något mindre effektiva i kombination med andra skyddsmetoder. Detta innebär inte nödvändigtvis att dessa skyddsmetoder bör undvikas, med det skall påpekas att för att ha ett skydd vilket enkelt kan byggas ut med fler ytterligare skyddsmetoder bör andra skyddsmetoder väljas.

Anledningen att SYN cookies är problematisk att kombinera med andra skyddsmetoder är att flera av dessa utnyttjar beteendet hos TCP för att minimera problemen med SYN flooding-attacker. SYN cookies ändrar detta beteende avsevärt. Då SYN cookies implementerats finns inte längre några halvöppna sessioner att stänga med RST-segment eller behovet för en datastruktur för hantering av sådana sessioner.

Nätverksbaserad lösning B, implementerad i offrets nätverk, är något problematisk att kombinera med andra. Den största anledningen till detta är hur metoden arbetar. Denna skyddsmetod bygger på att en attack upptäcks av offret. Upptäckt av en inkommande attack kan eventuellt försvåras om SYN cookies används, då ingen data sparas kring mängden inkommande SYN-segment. Detta kan naturligtvis lösas genom att exempelvis implementera en ytterligare detektor hos offret. En sådan kombination tycks dock överdrivet komplicerad. Nätverksbaserad lösning A, implementerad vid angriparens nätverk, syftar till att upptäcka utgående attacker. Förvisso kan dessa två kombineras till viss grad, men i stort blir problematiken tämligen lik den tidigare diskuterad mellan SYN cookies och SYN cache. Skulle attacken inte kunna upptäckas, och stoppas, vid angriparens nätverk så kan nätverksbaserad lösning B agera vidare. Dessa kan dock inte kallas kompatibla då de inte ökar effektiviteten då de implementeras parallellt.

Den brandväggsbaserade skyddsmetod som undersökts, presenterad av Schuba et al.(1997), förväntas inte arbeta helt effektivt i kombination med den nätverksbaserad lösning C, presenterad av Safa et al. (2007), implementerad vid det spoofade nätverket. Anledningen till detta är att de båda skyddsmetoderna arbetar genom att generera RST-segment för att stänga halvöppna session hos offret. Detta beteende blir således i stort redundant. Möjligheten finns att andra brandväggsbaserade lösningar existerar, vilka är mer kompatibla med nätverksbaserad lösning C.

Vid val av vilka skyddsmetoder som bör väljas för implementation måste dessutom hänsyn tas till effektivitet hos de individuella skyddsmetoderna. En mycket effektiv kombination av ineffektiva skyddsmetoder är inte nödvändigtvis sammantaget effektiv.

8 Utvärdering av skyddsmetoder med hänsyn till eventuella krav

Somliga organisationer lider större risk att utsättas för DoS-attacker, beroende på exempelvis att de är involverade i kontroversiella frågor eller att de innehar en stor mängd Internet-baserade tjänster. Andra organisationer kan vara något mindre attraktiva mål, men har höga krav på tillgänglighet av de tjänster som riskeras utsättas för en attack. Det är i huvudsak för dessa typer av organisationer det är önskvärt att implementera ett sammansatt skyddspaket för att i mesta möjliga mån kunna stoppa attacker eller minimera skadan dessa skapar. Organisationer mot vilka hotbilden är mindre riskerar i mycket liten utsträckning att utsättas för någon mer omfattande attack, och därmed bör en ensam skyddsmetod vara tillräckligt skydd.

SYN cache förväntas vara mycket effektivt för att hantera mindre attacker samt bör även fungera väl i kombination med närmast samtliga andra skyddsmetoder. Detta, tillsammans med den förhållandevis enkla implementationen i system där möjlighet finns att aktivera funktionen i operativsystemets kärna, talar starkt för att SYN cache bör användas närhelst detta är möjligt. Liksom SYN cache implementeras SYN cookies lokalt på den maskin mot vilken en hotbild finns. Detta medför att om stöd finns i operativsystemet för en sådan implementation bör denna vara förhållandevis enkel att åstadkomma.

Som visats i föregående kapitel finns goda möjligheter att utöver SYN cache implementera ytterligare skyddsmetoder. För SYN cookies är dessa möjligheter något mer begränsade. Det är dock mycket viktigt att inse att om möjlighet att använda en SYN cache inte finns, men SYN cookies är möjligt att aktivera rekommenderas detta varmt. Som visat av Lemon (2002) ger också, med reservation för eventuella förändringar i det fall ytterligare skyddsmetoder skulle användas, SYN cookies förbättrad verkningsgrad som komplement till SYN cache. Sannolikt är denna förbättrade verkningsgrad i förhållande till kostnad för implementation inte motiverad om möjlighet finns att implementera andra skyddsmetoder.

Beroende på vilken typ av brandväggsbaserad lösning som väljs kan en sådan dessutom vara mycket effektiv i kombination med andra skyddsmetoder. En brandvägg kan då skydda flera utsatta tjänster om så krävs. Ett naturligt steg för en växande organisation skulle kunna vara att en successiv implementation av allt fler skyddsmetoder för att nå ett mer effektivt skydd. Det mest lovande tillvägagångssättet för detta skulle stegvis kunna beskrivas som följer:

1. Förstärk TCP/IP-stacken lokalt på de utsatta tjänsterna, genom att konfigurera en väl vald time-out för halvöppna sessioner samt en lagom storlek på backlogen.
2. Aktivera skyddsmetoder lokalt på den tjänst som skall skyddas, exempelvis SYN cache eller SYN cookies om dessa finns tillgängliga i det operativsystem som används.
3. Installera en brandväggslösning vilken kan skydda samtliga tjänster som riskerar utsättas för attacker. Val av typ av brandvägg bör göras så att denna är kompatibel med eventuellt skydd implementerat tidigare. Exempelvis skulle en brandvägg av typen relay (se kapitel 6.4) förgöra syftet med SYN cache på de utsatta maskinerna då backlogen på dessa aldrig kommer utsättas för en SYN flood. I det fall en brandvägg inte anses tillräckligt samt att organisationen i frågas nätverk inte är stort nog för implementation av en nätverksbaserad skyddsmetod bör flera lager av brandväggsbaserade lösningar kunna kombineras. Beroende på faktorer som funktionalitet hos dessa samt trafikflöde finns dock en viss risk att för märkbar prestandaförlust.
4. Implementera någon form av överliggande nätverksbaserat skydd för att blockera attack-trafik. Detta steg kan inte realistiskt genomföras inom organisationer vars interna nätverk inte är stort nog att självt innehålla flera nätverkssegment separerade av routrar på vilka en sådan lösning kan verka. Vilken nätverksbaserad metod som bör väljas är högst beroende på utseendet av organisationens nätverk.

De skyddsmetoder presenterade av Safa et al. (2007), Wang et al. (2002a), Wang et al. (2002b) samt Internet Engineering Task Force (2002a) skyddar inte direkt implementatörens egna tjänster.

Utöver tidigare nämnda rekommendationer kan många fördelar identifieras med en gemensam ansats hos en större mängd organisationer. Flera skyddsmetoder skyddar inte sin implementationsplats utan används för att antingen hindra utgående attacker eller mildra effekterna av attacker mot andra mål. Den egna vinsten av att implementera dessa är avsevärt mycket svårare att motivera, främst finansiellt. Dock finns vinster att göra såväl i goodwill samt genom att minska intresset för att genomföra SYN flooding-attacker då dessa skulle vara betydligt mindre effektiva.

Enligt Tabell 1 förväntas samtliga undersökta skyddsmetoder vara effektiva i hanteringen av mindre attacker. Det är viktigt att inse att skillnaden mellan en oskyddad tjänst och en tjänst där en godtycklig skyddsmetod implementerats kan förväntas vara mycket stor.

9 Reflektioner

Somliga skyddsmetoder (Safa et al., 2007; Internet Engineering Task Force 2000a; Wang et al., 2002a; Wang et al., 2002b) syftar främst eller endast till att hindra attacker från att utgå från det nät där dessa implementeras. Generellt antas att motivationen för att implementera dessa är lägre än för de skyddsmetoder som skyddar implementatörens egna tjänster från attacker. Viss motivation kan fås gällande skyddsmetoden presenterad av Safa et al. (2007) genom hur denna avvärjer den sekundära DoS-attack som diskuteras i kapitel 6.5.3. Metoder som implementeras närmare en angripare kan dock ha somliga fördelar gällande upptäckt samt motverkan av attacker då det kan vara enklare att upptäcka onormalt beteende nära angriparen än vid offrets ände. Detta beror på att normalt trafikflöde hos offret sannolikt är tämligen likt en SYN flooding-attack, det vill säga att den består av inkommande förfrågningar från en mängd olika avsändare. Utgående trafik från ett nät bör dock sällan i normalfallet innehålla avsändaradresser på andra nät i fallet filtrering, eller bestå av en enorm mängd utgående förfrågningar. Metoder som undersöker mängden utgående förfrågningar kan kringgås med hjälp av en lågintensiv distribuerad attack från en stor mängd maskiner på nätverket Wang et al. (2002a) samt Wang et al. (2002b) visar dock att den metod som presenteras kan upptäcka attacker redan vid mycket små mängder SYN-segment vilka inte bidrar till uppstartade sessionen. Det är dessutom betydligt enklare att spåra angriparen om attacken upptäcks nära ursprunget.

Generellt bör internetleverantörer ha ett intresse av att begränsa mängden DoS-attacker av samtliga slag, såväl från som till det egna nätverket. Detta då inkommande attacker kan innebära försämrat förtroende hos kunderna samt såväl inkommande som utgående attacker konsumerar, en troligtvis inte trivial mängd, bandbredd vilket försämrar nätverkets prestanda. Att implementera filtrering för att tidigt kunna kasta IP spoofad trafik kan innebära en förbättring av övergripande nätverksprestanda. Dessutom antas att anseendet hos andra internetleverantörer stiger för dem som aktivt motarbetar kriminella handlingar gentemot deras kunder.

Ett intressant scenario vore en fullständig implementation av nätverksbaserad lösning B över hela det publika Internet. Med en hierarkiskt segmenterad struktur bör attacker kunna stoppas vid källan, och därmed också tämligen enkelt kunna härledas till specifika maskiner. Sannolikt skulle detta innebära en viss overhead dock.

Under arbetets gång har inga särskilda svårigheter påträffats. Det mest problematiska har varit att lokalisera relevanta skyddsmetoder. De skyddsmetoder som valts ut har i mesta möjliga mån valts för att representera klasser av skyddsmetoder. Att välja dessa med minimalt överlapp utan att för den skull förlora relationer till andra möjliga skyddsmetoder var inte helt trivialt.

En punkt i detta arbete som är öppen för debatt är de egenskaper som listats i kapitel 6.6. De egenskaper som tagits fram bör vara av intresse och de betyg som tilldelats respektive skyddsmetoder bör vara tämligen korrekta. Somliga egenskaper, vilka kan vara av intresse, kan dock ha utelämnats.

10 Uppslag för vidare arbete inom området

Detta arbete har visat att skyddsmetoder finns vilka effektivt begränsar problemet från SYN flooding. Det saknas dock mer djupgående studier och praktisk testning. Vidare, framförallt praktisk, undersökning av såväl individuella skyddsmetoder i jämförelse samt kombinationer av skyddsmetoder är ett område inom vilket mer arbete behövs.

Undersökningar bör göras, i det fall sådana inte redan existerar, kring varför en övergång från TCP till SCTP inte ännu skett på bred front. En sådan övergång skulle omöjliggöra SYN flooding.

Brandväggsbaserade och nätverksbaserade lösningar finns i många olika varianter. En vidare kartläggning på vardera av dessa områden kan vara av intresse för de som planerar att genomföra steg 3 och 4 presenterade i kapitel 8.

En argumentation bör göras på ett internationellt plan för standardisering av någon skyddsmetod. Samtliga presenterade i detta arbete anses relativt en oskyddad maskin vara mycket effektiva. Det anses att det är av större vikt att införa en standard vilken kan följas och vilken är någorlunda effektiv än att lämna tjänster oskyddade i väntan på en mer effektiv skyddsmetod.

TCP tycks befästa sin plats som en del av grunden till elektronisk kommunikation och ett hot av en magnitud som SYN flooding kan därmed anses vara ett hot mot elektronisk kommunikation i dess helhet.

Referenser

Cohen, F (1996). *Internet Holes – Part 13: The SYN Flood.* Elsevier Science Ltd.

Douligeris, C., Mitrokotsa A. (2004). DDoS attacks and defense mechanisms: classification and state-of-the-art, *Computer Networks 44* (2004), 643-666

Halsall, F. (2005). *Computer Networking and the Internet, 5th ed.* Harlow: Pearson Education Limited.

Hansson, A. (2010). *Västgöta-Data AB*. Personlig kommunikation 2010-02-18.

Harris B., Hunt R. (1999). TCP/IP security threats and attack methods, *Computer Commuications 22* (1999), 885-897.

Internet Engineering Task Force (1980). *User Datagram Protocol.* Request For Comments 768. Tillgänglig på Internet: http://tools.ietf.org/html/rfc768 [Hämtad 2010-03-10].

Internet Engineering Task Force (1981). *Transmission Control Protocol.* Request For Comments 793. Tillgänglig på Internet: http://tools.ietf.org/html/rfc793 [Hämtad 2010-03-10].

Internet Engineering Task Force (2000a). *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing,* Request For Comments 2827. Tillgänglig på Internet: http://tools.ietf.org/html/rfc2827 [Hämtad 2010-03-10].

Internet Engineering Task Force (2000b). *Stream Control Transmission Protocol.* Request For Comments 2960. Tillgänglig på Internet: http://tools.ietf.org/html/rfc2960 [Hämtad 2010-03-10].

Internet Engineering Task Force (1998). *Reverse Tunneling for Mobile IP, revised*, Request For Comments 3024. Tillgänglig på Internet: http://tools.ietf.org/html/rfc3024 [Hämtad 2010-03-10].

Internet Engineering Task Force (2002). *IP Mobility Support for IPv4*, Request For Comments 3220. Tillgänglig på Internet: http://tools.ietf.org/html/rfc3220 [Hämtad 2010-03-10].

Internet Engineering Task Force (2007). *TCP SYN Flooding Attacks and Common Mitigations.* Request For Comments 4987. Tillgänglig på Internet: http://tools.ietf.org/html/rfc4987 [Hämtad 2010-03-10].

Lemon J. (2002). Resisting SYN flooooding DoS attacks with a SYN cache. *Proceedings of USENIX BSDCon '02 conference on file and storage technologies, February* (2002), 89-98.

Ohsita Y, Ata S, Murata M. Deployable overlay network for defense against distributed SYN flood attacks. *Proceedings of the 14th international conference on computer communications and networks* (2005), 407–412.

Safa, H., Chouman, M., Artail, H., Karam, M. (2007). A collaborative defense mechanism against SYN flooding attacks in IP networks. *Journal of Network and Computer Applications 31* (2008), 509–534.

Schuba C-H, Krsul I-V, Khan M-G, Spafford E-H, Sundaram A, Zamboni D. (1997). Analysis of a denial of service attack on TCP. *Proceedings of the IEEE symposium on security and privacy* (1997), 208–223.

Tupakula U-K, Varadharajan V, Gajam A-K. (2004). Counteracting TCP SYN DDoS attacks using automated model. *Proceedings of IEEE the Global Telecommunications Conference (GLOBECOM ’04)* (2004), 2240–2244.

Wang H, Zhang D, Shin K. (2002a). Detecting SYN flooding attacks. *Proceedings of the twenty-first annual joint conference of the IEEE computer and communications societies.* (2002b), 1530–1539.

Wang H, Zhang D, Shin K. (2002b). SYN-dog: sniffing SYN flooding sources. *Proceedings of the 22nd International Conference On Distributed Computing Systems (Icdcs'02)* (2002), 421–428.

Xiao B., Chen W., He Y. (2008). An autonomous defense against SYN floooding attacks: Detect and throttle attacks at the victim side independently. *Journal of Parallel Distributed Computing 68* (2008), 456-470.

Zuquete A. (2002). Improving the functionality of SYN cookies. *Proceedings of 6th IFIP communications and multimedia security conference* (2002), 57–77.