Peer-to-Peer säkerhet

Kasper Gustafsson

Examensarbete

Informationsteknik

2016

EXAMENSARBETE	
Arcada	
Utbildningsprogram:	Informations- och medieteknik
Identifikationsnummer:	5838
Författare:	Kasper Gustafsson
Arbetets namn:	Peer-to-Peer säkerhet
Handledare (Arcada):	Jonny Karlsson
Uppdragsgivare:	Självständigt arbete

Sammandrag:

Arbetets område är Peer-to-Peer säkerhet och baserar sig på litteraturstudier. Ett Peer-to-Peer nätverk är ett datornätverk av sammankopplade noder som inte följer klient-server modellen. Noderna i nätverket kan agera i alla roller, vilket leder till att noderna kan kommunicera direkt med varandra utan behov av en server. En enhet kan fritt ansluta sig till ett P2P-nätverket, detta gör nätverket mycket sårbart eftersom skadliga enheter kan vara svåra att skilja från vanliga enheter. Olika skyddsmekanismer kan användas för att skydda sig mot specifika attacker men oftast är det väldigt svårt att fullständigt skydda sig eftersom ett P2P-nätverk oftast är öppet för vem som helst. Arbetet kommer ta upp vad P2P-säkerhet är, populära P2P attacker, hur man skyddar sig mot dessa attacker och hur man överlag skyddar sig på internet. Materialet som använts är olika forskningspapper kring området som presenterats på olika tillfällen. Arbetet går inte in på hur alla P2P-nätverk är uppbyggda utan begränsar sig till säkerhetsattackerna och hur man skyddar sig mot dem.

Nyckelord:	Peer-to-Peer, P2P, nätverk, säkerhet, internet, attacker, åtgärder
Sidantal:	28
Språk:	Svenska
Datum för godkännande:	

DEGREE THESIS	
Arcada	
Degree Programme:	Information and Media Technology
Identification number:	5838
Author:	Kasper Gustafsson
Title:	Peer-to-Peer security
Supervisor (Arcada):	Jonny Karlsson
Commissioned by:	Independent work

Abstract:

The area of this work is P2P security and it is based on literature studies. A Peer-to-Peer network is a computer network of interconnected nodes that do not follow the client-server model. The nodes in the network can act in all the needed roles, which leads to that the nodes can communicate directly with each other without the need for a server. A device can freely join a peer-to-peer network, this makes the network very vulnerable as it can be difficult to distinguish bad units from normal units. Different security mechanisms can be used to protect against specific attacks, but usually it is very difficult to completely oneself in a peer-to-peer network as the network is open to anyone. This paper will focus on what P2P security is, popular P2P attacks, how to protect against these attacks and how to generally protect oneself on the internet. The material used are different research papers on the area presented on various occasions. The purpose and goal is to provide the reader with information about P2P, P2P security, P2P attacks, how to protect against the attacks and how to generally protect on self on the internet. The work will not go into how all the P2P networks are built but will rather focus on the security attacks and how to protect against them.

Keywords:	Peer-to-Peer, P2P, network, security, internet, attacks, countermeasures
Number of pages:	28
Language:	Swedish
Date of acceptance:	

INNEHÅLL

Figurer

Tabeller

FÖRKORTNINGAR

P2P	Peer-to-Peer
DoS	Denial-of-service
DDoS	Distributed denial-of-service
VPN	Virtual private network
ISP	Internet service provider (Internetleverantör)
ID	Identifier

1 INLEDNING

Ett P2P (Peer-to-Peer) nätverk är ett datornätverk av sammankopplade noder som inte följer klient-server modellen. I ett P2P-nätverk kan alla noder agera i alla roller, vilket leder till att noderna kan kommunicera direkt med varandra utan behov av en server. I dagens läge används P2P-teknologi för det mesta i fildelningsprotokoll som BitTorrent och Dropbox, såväl som i snabbmeddelande kommunikationssystem såsom Skype.

Ett P2P-nätverk kan också vara ett billigare alternativ för företag eftersom man inte behöver skaffa skilda servrar som styr trafiken, men detta kan också orsakar flera säkerhetsrisker.

1.1 Bakgrund

Inom P2P-nätverk så som i alla andra nätverk finns det säkerhetshot som är allvarliga med tanke på användningen. En enhet kan fritt ansluta sig till ett P2P-nätverket, detta gör nätverket mycket sårbart eftersom skadliga enheter kan vara svåra att skilja från vanliga enheter. En skadlig enhet kan attackera nätverket på många olika sätt, en av de vanligaste attackerna är en DoS attack som försöker översvämma nätverket med falska paket för att hindra trafik i nätverket. Olika skyddsmekanismer kan användas för att skydda sig mot specifika attacker men oftast är det väldigt svårt att fullständigt skydda sig eftersom ett P2P-nätverk oftast är öppet för vem som helst. Arbetet kommer fokusera sig på säkerhetssidan inom P2P.

1.2 Syfte och mål

Syftet med arbetet är att redogöra för vad P2P egentligen är och dess användningsområden i dagens läge. Fokus sätts vid säkerhetsproblem inom P2P samt en utvärdering av existerande säkerhetslösningar.

Frågor som kommer att besvaras:

- Vad är P2P?

- Hur skiljer sig P2P från klient-server modellen?
- Vad är P2P säkerhet?
- Vad är en P2P attack?
- Vad finns det för säkerhetshot som är specifika för P2P-nätverk?
- Vad finns det för skyddsåtgärder mot P2P säkerhetshot och hur väl fungerar de?

1.3 Avgränsningar

Arbetet kommer inte ta upp exakt alla säkerhetsattacker det finns mot P2P-nätverk eftersom det finns så många olika, däremot kommer arbetet att fokusera sig på de populäraste attackerna. Arbetet kommer nämna några olika P2P-nätverkstyper och när de grundades, men kommer inte gå igenom dem desto djupare.

1.4 Metoder

Arbetet baserar sig på olika litteraturstudier. Litteraturen innehåller en bok om P2P och flera forskningspapper som fokuserar sig på P2P attacker och åtgärder, forskningspappren har presenterats på olika tillfällen. Litteratur som tar upp säkerhetsattacker och motgärder i P2P-nätverk finns det mycket begränsat av, så årtalen kan hoppa från 2000-talets början till 2016.

Arbetet är indelat i sex kapitel. Kapitel två tar upp vad ett P2P-nätverk är och hur det skiljer sig från ett klient-server nätverk. Kapitel tre beskriver vad P2P attacker är för något och ger mer information om några specifika attacker. Kapitel fyra redogör vilka olika motåtgärder man kan använda för att skydda sig emot attackerna som tagits upp i tredje kapitlet. Kapitel fem tar upp vilka olika skyddsmetoder en användare kan använda för att skydda sig själv eller viktig information över nätet. Kapitel sex behandlar resultaten. Här redogörs hur arbetet motsvarar de ursprungliga målen. Besvarar arbetet de frågor vi ställde i början och vilka eventuella brister den har. Kapitel sju tar upp slutsatser.

2 PEER-TO-PEER

Internet som ursprungligen skapades var ett P2P system. Det fanns inga brandväggar så säkerheten var väldigt låg. Alla maskiner på internet kunde skicka paket till varandra. De säkerhetsintrång som förekom var väldigt få samt ofarliga. (Oram 2001 s. 9)

Kring 1979 skapades det första systemet som liknade P2P-arkitektur, ett distribuerat system för meddelanden som hette USENET. USENET använde sig av en decentraliserad modell och sägs vara på vissa sätt basen för P2P applikationerna Gnutella och Freenet. (Oram 2001 s. 9-10)

P2P blev populärt på 1990-talet för delning av multimedia filer. Tabellen nedan visar populära P2P protokoll och när de skapades (Jaideep & Prakash Battula 2016 s. 1).

Tabell 1 Populära P2P protokoll

P2P protokoll	Utgivningsår
Freenet	Juli 1999
Napster	September 1999
Direct Connect	November 1999
Gnutella	Mars 2000
BitTorrent	April 2001

Napster, som skapades 1999 av Shawn Fanning var början på de P2P-nätverk vi känner idag. Napster var ett P2P-fildelningsprogram var användarna bildade ett virtuellt nätverk som var helt oberoende av det fysiska nätverket och inte behövde lyda några begränsningar. Napster skiljer sig dock lite från andra P2P-nätverk eftersom Napster använder en central server som sparar information om vilka användare som delar vilka filer. Så om en användare vill ha en viss fil så gör användaren en förfrågan till servern som sedan svarar vilken användare som har filen tillgänglig.

P2P-nätverk såsom BitTorrent, Napster, Gnutella och Freenet är några av de existerande programmen som i dagens läge gör det möjligt för användarna att dela och söka efter resurser (Jaideep & Prakash Battula 2016 s. 1).

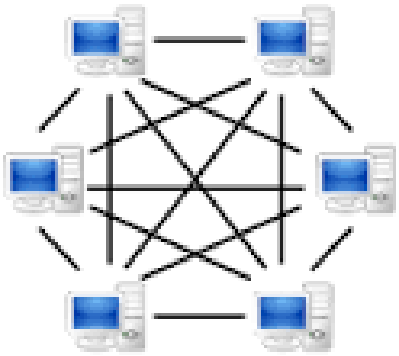
2.1 Vad är Peer-to-Peer

P2P-nätverk skiljer sig från ett traditionellt klient-server datornätverk. Klient-server nätverk använder sig av en eller flera servrar som är dedikerade till att erbjuda tjänster till kunderna. Ett P2P-nätverk är inte beroende av servrar utan alla noder i ett P2P-nätverk kan själva fungera som server eller klient. (Jaideep & Prakash Battula 2016 s. 1)

Ett P2P-nätverk kan klassificeras som ett öppet nätverk, alla användare kan lätt ansluta sig till eller lämna nätverket. Eftersom varje användare i ett P2P-nätverk själva fungerar som server och klient ger det vissa fördelar, bättre lastbalansering, självorganisering, feltolerans och förmågan att samla och utnyttja stora mängder resurser. (Vroonhoven 2006 s. 1)

2.2 Peer-to-Peer vs Klient-server

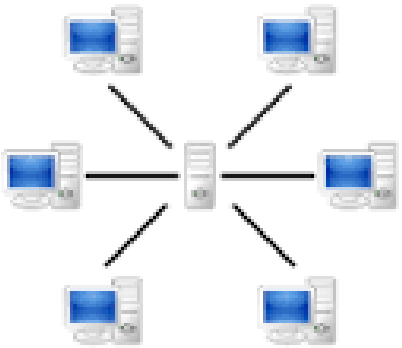
I figur 1. ser vi hur ett P2P-nätverk är uppbyggt. Alla noder är kopplade med varandra utan behov av en server.



Figur 1. Ett P2P-nätverk av sammankopplade noder

Figur 2 visar hur ett klient-server nätverk är uppbyggt. Alla data som skickas mellan noderna går igenom en server. En server har oftast ett jobb, en webbserver arbetar med webbsidor medan en filserver arbetar med att skicka datafiler men det är också möjligt

för en server att kunna göra flera jobb samtidigt som t.ex. fungera både som en webbserver samt filserver.



Figur 2. Ett nätverk baserat på klient-server modellen

Ett P2P-nätverk har både fördelar och nackdelar jämfört med ett klient-server nätverk. P2P-nätverk är ett billigare alternativ eftersom man inte behöver skaffa en skild server och kan därför vara ett bra alternativ för t.ex. ett litet företag med färre datorer. P2P-nätverk behöver mjukvara för att kunna ansluta sig till varandra. Så varje dator som vill ansluta sig till ett nätverk behöver rätt mjukvara installerat istället för att man installerar allt på en och samma server som i ett klient-server nätverk.

Resurserna av datorerna i ett P2P-nätverk kan också lätt bli överbelastade eftersom de inte bara måste stöda arbetsstationens användare utan också alla förfrågningar som kommer från andra nätanvändare.

3 PEER-TO-PEER ATTACKER

Eftersom ett P2P-nätverk är så öppet kan en skadlig användare ansluta sig till nätverket lika lätt som en vanlig användare. Vanliga användare kan därför råka ut för olika säkerhetsattacker. (Vroonhoven 2006 s. 1)

DoS attack, DDoS attack och man-i-mitten attack som tas upp i detta kapitel är inte bara begränsade till P2P-nätverk utan förekommer också i andra nätverk. De andra attackerna är specifika för P2P-nätverk. (Yang & Yang 2012 s. 1-5)

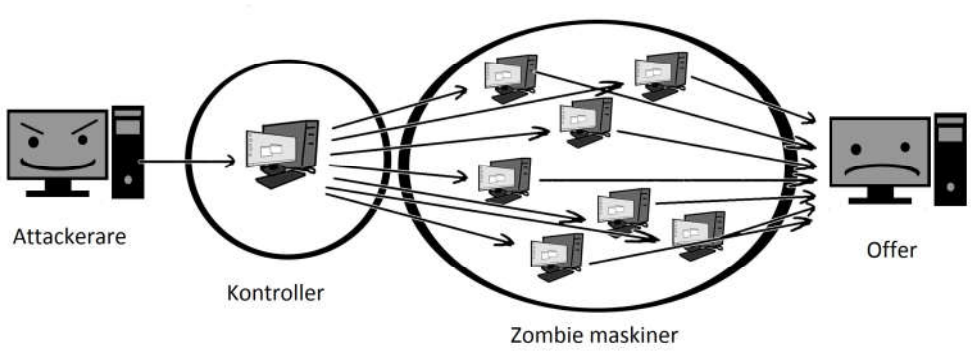
3.1 DoS attack

En DoS-attack är en attack mot en dator eller ett nätverk som försöker göra en datorresurs otillgänglig för dess tänkbara användare. I ett P2P-nätverk är den vanligaste DoS attacken ett försök att översvämma nätverket med falska paket för att hindra normala användare från att nå den data de vill nå. En annan metod är att försöka dränka offernoden med falska begäran så att noden blir alltför upptagen för att kunna svara på andra frågor som kommer från normala användare. (Yang & Yang 2012 s. 1)

För Napster som använder sig av en central server som tar emot sökfrågor från användare kan en DoS-attack vara ett mycket större problem. Attacken kan fokusera sig på servern som sedan kan leda till att hela nätverket låser sig. (Wang 2016 s. 3)

3.2 DDoS attack

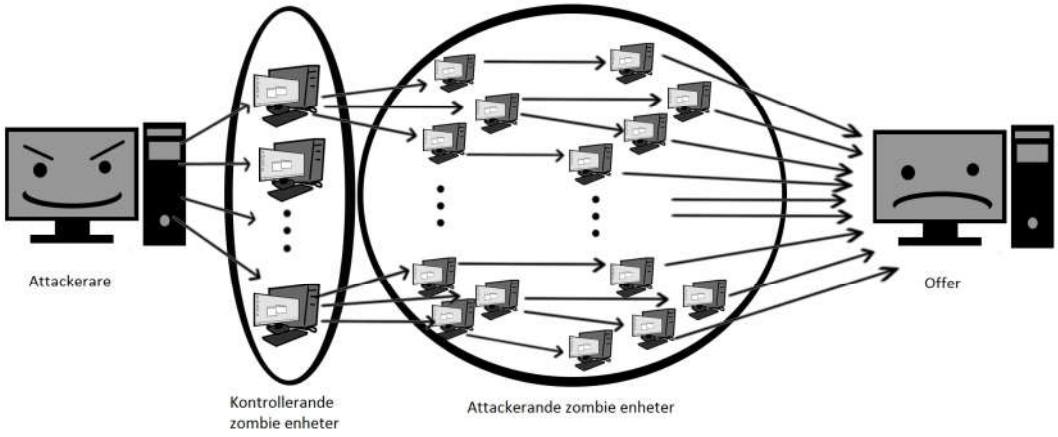
En DDoS attack är en attack som är baserad på en DoS-attack. En DDoS-attack kan delas upp i fyra olika steg. Figur 3 visar uppbyggnaden av en DDoS-attack.



Figur 3. Strukturen av en DDoS-attack

Attackeraren styr kontrollenheten och zombie maskinerna. Kontrollenheten och zombie maskinerna är oftast personliga datorer med bredbandsanslutning som har blivit utsatta för ett virus eller en trojan. Skillnaden mellan kontrollenheten och zombie maskinerna är att attackerna mot offret endast kommer från zombie maskinerna. Kontrollenheten tar endast emot en attack order från attackeraren som den sedan skickar vidare till zombie maskinerna utan att själv delta i attacken mot offret. (Yang & Yang 2012 s. 1-2)

En DDoS-attacks detaljerade delar kan också utvecklas på olika sätt. Figur 4 visar ett exempel på en utvecklad DDoS-attack.



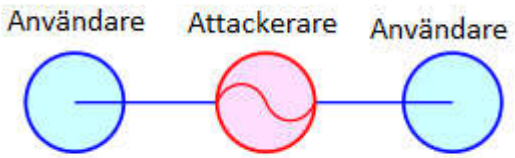
Figur 4. Exempel på en utvecklad DDoS-attack

I detta exempel kontrollerar attackeraren flera kontrollenheter, attackeraren skickar en attack order till varje kontrollenhet. Kontrollenheterna skickar attack ordern vidare till zombie enheterna som sedan attackerar offret. Detta gör det ännu svårare att få tag på attackeraren eftersom attackeraren oftast är indirekt inblandad. (Yang & Yang 2012 s. 2)

3.3 Man-i-mitten attack

En man-i-mitten attack är ett indirekt intrång, var attackeraren placerar sin datorenhet oupptäckt mellan två noder. Efter attackeraren gjort sitt intrång kan attackeraren fånga upp och ändra meddelanden som skickas mellan två normala användare utan att användarna vet om det. (Jaideep & Prakash Battula 2016 s. 3)

Figur 5 visar strukturen av en man-i-mitten attack.



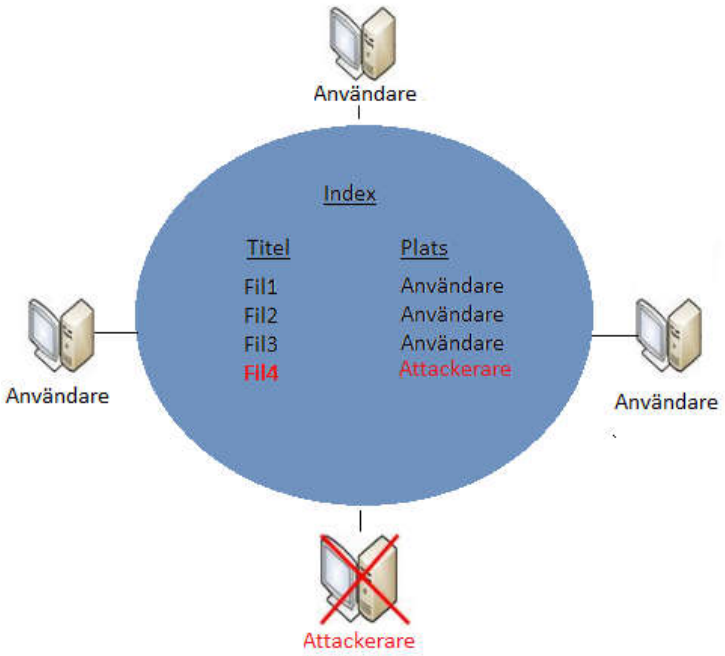
Figur 5. Exempel på en man-i-mitten attack

3.4 Index förgiftningsattack

De flesta P2P-fildelnings system använder sig av ett index, vilket gör det lätt för en användare att hitta önskat innehåll. En förgiftningsattack siktar sig på en användares index förfrågan som sedan gör det svårt att hitta rätt innehåll. Attackeraren sätter in en stor mängd av ogiltiga enhetsinformationer in i indexet som orsakar svårigheter för användaren att hitta rätt innehåll. (Yang & Yang 2012 s. 4)

BitTorrent är ett exempel som lätt kan råka ut för förgiftningsattacker. I BitTorrent laddar man först ner en fil med förlängningen .torrent. Filen innehåller information som storleken på filen, namnet på filen och en tracker. Med trackern tar man reda på vilka andra enheter som också försöker nå samma fil. När en enhet påbörjar en uppgift om en BitTorrent fil annonseras det till trackern, efter det kan trackern sedan nå information om andra enheter som är länkade till samma fil. Problemet här är att när trackern sedan får sin information om de andra enheterna så autentiserar den inte ifall innehållet verkligen är tillgängligt. Så attackeraren kan annonsera en stor mängd information om ogiltiga enheter. När en användare sedan försöker hämta filen från den informationen trackern hämtat är det en stor chans att användaren inte når andra riktiga användare utan istället når en ogiltig enhet. (Yang & Yang 2012 s. 4)

Figur 6 demonstrerar hur ett index med ogiltiga enheter kan se ut.

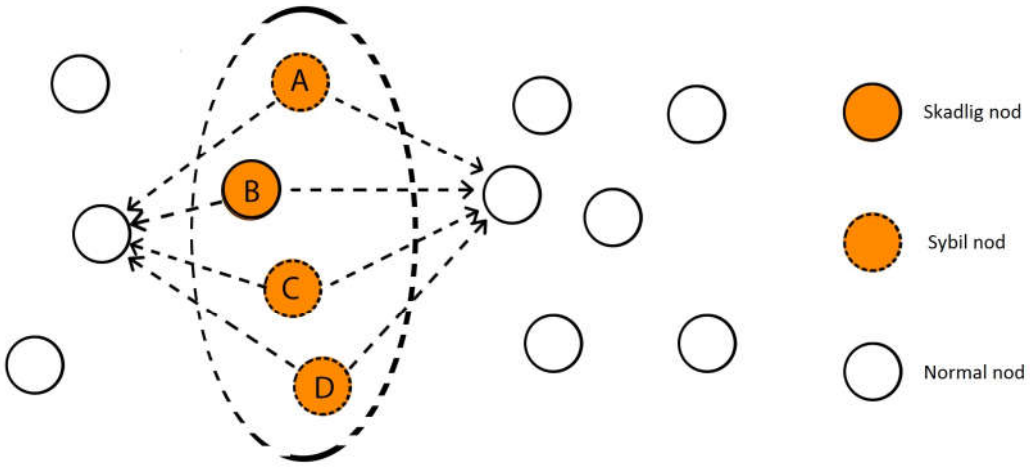


Figur 6. Exempel på ett index som drabbats av en ogiltig enhet

3.5 Sybil attack

Ett P2P-nätverk kan erbjuda en redundant säkerhetskopieringsmekanism för att skydda en enhets integritet och privatliv. Varje enhet i ett P2P-nätverk har en egen ID, det är nätverkets uppgift att se till att alla enheter bara har en ID. En sybil attack sker då en attackerare ansluter sig till nätverket och representerar flera än en enhet, detta leder sedan till att enheten kan kontrollera en stor del av nätverket. (Yang & Yang 2012 s. 4)

Figur 7 visar uppbyggnaden av en sybil attack.



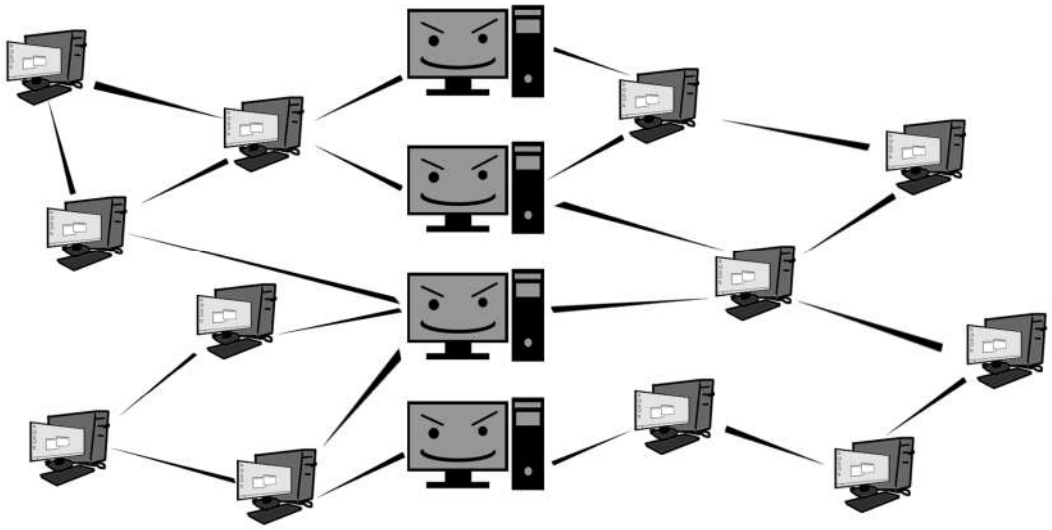
Figur 7. En sybil attack

I bilden ovan försöker en vit normal nod göra en säkerhetskopia. Den väljer en grupp enheter som i detta fall är A, B, C och D. Men noderna A, C och D existerar inte eftersom de är de skadliga noderna som nod B skapat och säkerhetskopieringen kan inte slutföras. (Yang & Yang 2012 s. 4)

3.6 Eclipse attack

En Eclipse attack är en vanlig attack i ett overlay nätverk. En attackerare kontrollerar en stor mängd onda noder som arbetar tillsammans för att lura goda noder. En god nod har en tabell var det finns information om nästa nod, i denna tabell skriver de onda noderna in sin adress. När en god nod sedan försöker skicka ett meddelande till nästa nod så kommer det att nå den onda noden istället. (Wang 2016 s. 5)

Figur 8 visar en eclipse attack var de onda noderna har separerat ett nätverk i två subnät.



Figur 8. En eclipse attack som har delat nätverket i två subnät

4 MOTÅTGÄRDER

P2P-nätverk saknar de säkerhetsverktyg som är tillgängliga för ett klient-server nätverk, så det är svårare att implementera säkerhetsskydd för ett P2P-nätverk. I ett klient-server

nätverk kan man sätta upp säkerhetsskydd rakt på servern och eftersom all trafik går igenom servern så skapas ett skydd för hela nätverket. I ett P2P-nätverk var man direkt är ansluten till en annan enhet istället för en server så måste varje enhet skyddas individuellt. Eftersom ett P2P-nätverk saknar viktiga säkerhetsverktyg så kan det vara svårt att skilja vänliga enheter ifrån skadliga enheter. (Friedman & Camp 2005 s. 2-3)

4.1 Motåtgärder för DoS attack

En teknik som allmänt används för att skydda sig mot DoS-attacker är prissättning. Denna teknik baserar sig på klient pussel protokollet (Client Puzzle Protocol). Protokollet är en datoralgoritm som skickar ett matematiskt pussel till alla användare som skickat en begäran åt servern. Användarna måste lösa pusslet före deras begäran svaras. Så när en attackerare försöker översvämma sitt offer med attacker måste pusslet lösas varje gång en ny attack skickas ut. Pusslet skall gå lätt att lösa men skall ändå kräva en minimal mängd beräkningar från klients sida. (Yang & Yang 2012 s. 1)

4.2 Motåtgärder för DDoS attack

Att skydda sig mot DDoS-attacker är väldigt svårt på grund av den stora mängden enheter som kan vara inblandade i en DDoS-attack. Man kan försöka övervaka den inkommande trafiken och svartlista den trafik man misstänker kan vara skadlig. Om ett företag ofta råkar ut för attacker kan man t.ex. ha ett säkerhetsteam övervaka inkommande trafik. (Jaideep & Prakash Battula 2016 s. 3)

Ett alternativ som har blivit populärt i dagens läge är att köra all sin trafik genom en VPN. Om en användare är ansluten till en VPN medan en attackerare försöker få tag på användarens IP-adress, når attackeraren bara VPN tjänstens IP-adress. När attackeraren sedan skickar attacker så drabbas VPN tjänsten av attackerna istället för användaren själv.

4.3 Motåtgärder för Man-i-mitten attack

Att skydda sig fullständigt emot en man-i-mitten attack är väldigt svårt. Det är rekommenderat att använda någon slags av krypteringsmetod för den information man skickar

ut. Om man krypterar sin information och en attackerare får tag på informationen så måste attackeraren kunna dekryptera det för att ha någon nytta av det. Ett annat alternativ är att använda sig av någon slags autentiserings teknologi. Autentiserarens uppgift är att verifiera att det verkligen är autentiserarens skapare som försöker ansluta sig eller skicka information utåt i nätverket. (Yang & Yang 2012 s. 2)

4.4 Motåtgärder för index förgiftningsattack

Det finns två specifika åtgärder som kan användas för att skydda sig mot index förgiftningsattacker. Det första alternativet är att autentisera versioner och fil annonser. En moderator kan gå igenom innehållet före det sätts upp för användning. Det andra alternativet är att låta användarna ranka källor. Om en källa skulle annonsera och ladda upp bra filer skulle den få en hög värdering, medan källor som laddar upp ogiltiga filer skulle få en låg värdering. (Yang & Yang 2012 s. 4)

4.5 Motåtgärder för sybil attack

För att skydda sig mot en sybil attack kan man använda sig av en identitets registrerings procedur som kallas självregistrering. En ny nod skapar en egen identifierare som innehåller nodens IP-adress och port. Identifieraren skickas sedan till färdigt registrerade noder. Efter identifieraren skickats ut så kan den nya noden skicka en begäran på att få ansluta sig till nätverket. Nu när de redan registrerade noderna fått informationen om den nya noden är det upp till dem att bestämma om den nya noden är falsk eller äkta. (Yang & Yang 2012 s. 4)

4.6 Motåtgärder för eclipse attack

Eftersom en eclipse attack baserar sig på en sybil attack kan samma motåtgärder användas. Om det inte är tillräckligt kan man övervaka antalet inkommande och utgående rutter från en nod. De inkommande rutterna kallas för indegree och de utgående rutterna kallas för outdegree. Eftersom varje nod i ett P2P-nätverk håller en tabell över sina grannoder

kan man hålla räkning på antalet inkommande och utgående rutter. Storleken på inkommande och utgående rutter avgör sedan om en eclipse attack håller på att ske. (Jaideep & Prakash Battula 2016 s. 4)

Ett annat alternativ är att ha alla noder skicka förfrågningar till grannodernas tabeller. Om sedan noden inte finns med på listan eller inkommande och utgående trafiken inte stämmer vet man att en eclipse attack pågår. (Wang 2016 s. 5)

5 ATT SKYDDA SIG PÅ INTERNET

Förutom att veta vad det finns för attacker och hur man skyddar sig mot dem är det bra att veta vad för säkerhetsprogram det finns till ens förfogande. Detta kapitel tar upp information om de vanligaste skyddsmetoderna och vad man skall tänka på när man söker efter de rätta skydden.

5.1 Virusskydd

Om man använder sig av en Windows maskin är man skyddad av Microsofts egna inbyggda virusskydd Microsoft Windows Defender. Tester har dock visat att det finns gratis virusskydd som erbjuder ett bättre skydd för din dator. (Rubenking 2016)

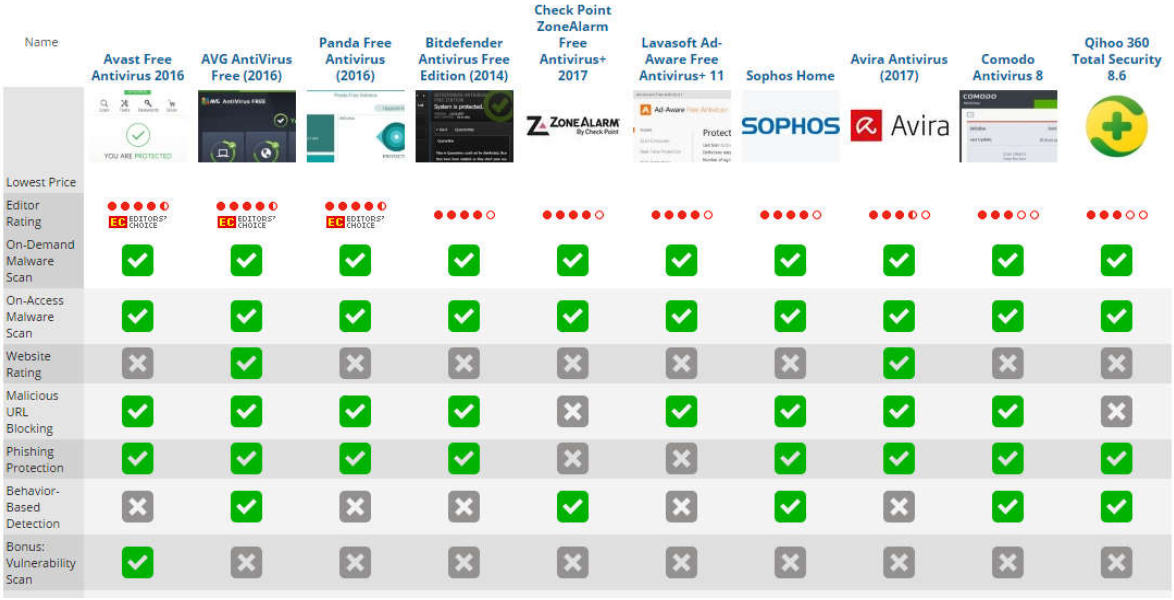
Ett virusskydd är en mjukvara som är designerad till att söka, upptäcka och ta bort mjukvaruvirus samt annan skadlig mjukvara som adware, trojander och maskar. Det finns många olika företag som erbjuder virusskydd. Medan de olika mjukvarorna erbjuder olika funktion erbjuder alla vissa grundläggande funktion:

- Skanna specifika kataloger eller filer för skadliga program
- Låter användaren planera skanningar som körs automatiskt
- Tar bort skadliga program som hittas
- Visar datorns ”hälsa”

Medan virusskydden ofta uppdateras automatiskt är det ändå bra för användaren att granska att mjukvaran är uppdaterat. (Criddle, u.å.)

Om man planerar att skydda eget företag är det alltid bättre att betala för ett skydd eftersom informationen man vill skydda oftast är väldigt viktig (Rubenking 2016). Virusskydd man betalar för erbjuder också teknisk telefonsupport, detta kan vara ytterst viktigt för företag med många maskiner (Quain 2016).

Figur 9 rankar gratis virusskydd. Man ser också vilka funktioner de olika gratisversionerna erbjuder.



Figur 9. Gratis virusskydd rankade av uk.pcmag.com

Figur 10 rankar betalda virusskydd

Figur 10. Betalda virusskydd rankade av uk.pcmag.com

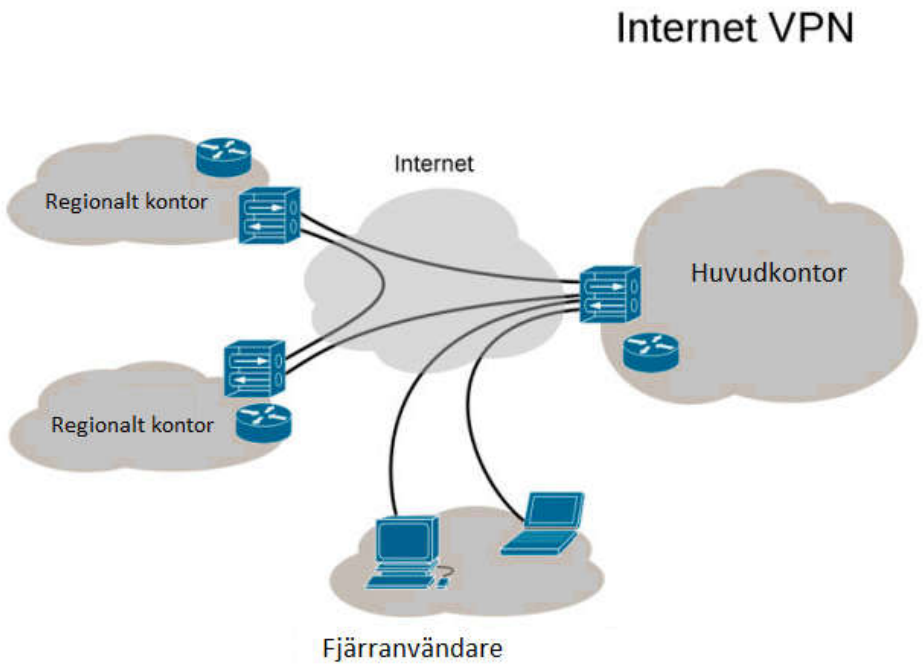
När det gäller grundläggande prestanda i att fånga skadlig mjukvara skiljer sig gratis och betalda virusskydd inte så mycket. Ett virusskydd man betalat för är dock bättre på att hitta och varna användaren om nya hot. (Quain 2016)

5.2 VPN

Vanligtvis när man ansluter sig till internet ansluter man sig först till sin ISP som sedan ansluter en vidare till de sidor man vill besöka. När man använder sig av en VPN ansluter man sig rakt till VPN servern istället för att först ansluta sig till sin ISP. (Crawford 2016)

All information som rör sig mellan användaren och VPN servern är krypterat, detta gör VPN ett populärt alternativ för företag som vill låta användare logga in på distans och även ansluta avlägsna datacenters. (Tarantola 2013)

I figur 11 ser vi ett exempel på hur ett företag skulle kunna sätta upp en VPN.



Figur 11. Exempel på ett företags VPN

I figuren ser vi hur fjärranvändare lätt kan ansluta sig till huvudkontoret från distans och hur regionala kontor kan ansluta sig med huvudkontoret och varandra.

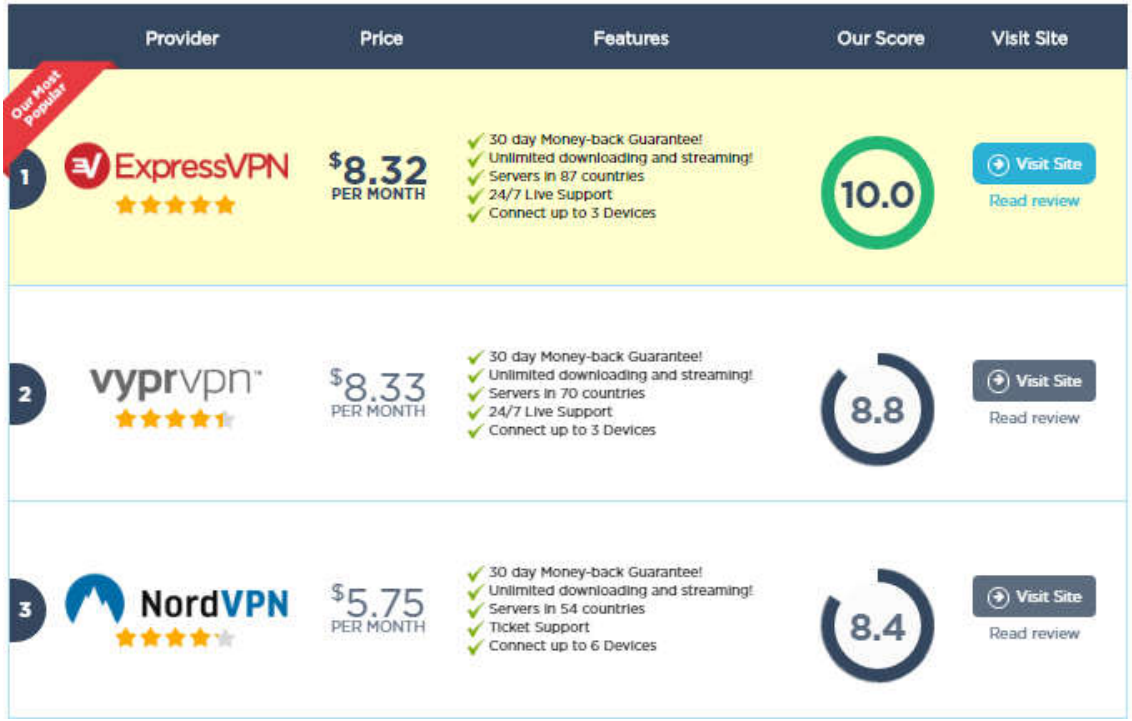
Användning av en VPN har ett antal viktiga konsekvenser (Crawford 2016):

1. All data som går via användarens egen dator och VPN servern är krypterat vilket gör att man kan använda internet helt privat.
2. Det ser ut som att användaren kommer åt internet från VPN-serverns IP-adress. Om man ansluter sig till en VPN-server som finns i ett annat land så ser det ut som man skulle vara ansluten från det landet. Användarens egen IP-adress är gömd, om någon övervakar din aktivitet kommer dom bara kunna spåra den tillbaka till VPN-servern.
3. Internethastigheten kommer att saktas ner eftersom information krypteras och dekrypteras. Men i dagens läge är skillnaden relativt liten given moderna datorer.
4. VPN leverantören vet dock vad du håller på med. Så med andra ord väljer man att lita på VPN leverantören istället för din ISP.
5. Användning av allmänna WiFi hotspots är mycket säkrare. Vanligtvis är det inte så säkert att ansluta sig till allmänna WiFi hotspots men eftersom egen information är krypterat så är det mycket säkrare.

Normalt kostar en VPN tjänst kring 5 - 10€ i månaden men det finns också en mängd gratis VPN tjänster. Gratis VPN tjänster är oftast starkt begränsade jämfört med betalda tjänster. (Crawford 2016)

Fast VPN nätverk har varit mest populärast inom företag har det på senaste tiden börjat bli allt mera populärt mellan vanliga användare p.g.a. orsakerna listat ovan. (Tarantola 2013)

Att välja rätt VPN beror på egna krav, var man att VPN servrarna skall finnas, vilka egenskaper man vill ha och kanske på priset. Figur 12 listar tre stycken populära VPN tjänster med leverantör, pris och egenskaper.



Figur 12. Populära VPN tjänster enligt bestvpn.com

5.3 Kryptering

Kryptering är en metod som skyddar personlig information från personer man inte vill att skall se det. Windows och Mac maskiner erbjuder inbyggda krypteringsverktyg som möjliggör kryptering för filer och hela partitioner. Windows krypteringsverktyg heter BitLocker och Mac maskinernas FileVault.

6 RESULTAT

Tabell 2 En översikt över attackerna

Attackens namn	Beteende	Försvarsstrategi	Farans omfattning	Försvarsnivån
DoS	1. Översvämmer nätverket med falska paket 2. Dränka offret med falska begäran	Prissättning	Medium	Lätt
DDoS	Attackeraren kontrollerar zombie enheter för att starta sin attack	Övervakning av inkommande trafik, svartlista trafik, användning av VPN	Hög	Svår
Man-i-mitten	Attackeraren placerar sig mellan två noder och fångar upp, modifierar och skickar data mellan två noder	Kryptera information, användning av autentiserings teknologi	Medium	Medium
Index förgiftning	Förgiftar index informationen som gör det svårt för noden att hitta rätt innehåll	Autentisering av versioner och filer, ranka källor	Hög	Medium
Sybil	Attacken kontrollerar ett antal enheter	Självregistrering	Hög	Svår
Eclipse	Skadliga noder arbetar tillsammans för att lura vanliga noder	Indegree och outdegree metod	Hög	Svår

Tabellen ovan listar resultaten som nåtts. Tabellen listar ut attackernas beteende, vilken försvarsstrategi bör användas, farans omfattning samt försvarsnivån. Farans omfattning är baserat på hur mycket en enhet eller ett nätverk påverkas av attacken. Om farans omfattning är hög kan en enhet eller hela nätverket drabbas så hårt att de blir helt oanvändbara. Försvarsnivån visar hur svårt det är att implementera de säkerhetsåtgärder som tagits upp.

7 SLUTSATSER

Ett P2P nätverk är ett datornätverk av sammankopplade noder som inte följer klient-server modellen. Alla noder i nätverket kan agera i alla roller, vilket leder till att noderna kan kommunicera direkt med varandra utan behov av en server. Skadliga enheter kan vara

svåra att skilja från vanliga användare eftersom en enhet kan fritt ansluta sig till de flesta P2P-nätverken. Olika skyddsmekanismer kan användas för att skydda sig mot specifika attacker men eftersom P2P-nätverk är så öppna kan det vara svårt att fullständigt skydda sig.

Syftet med arbetet är att redogöra vad P2P egentligen är och efter det ta upp populära säkerhetsattacker, vilka skyddsmetoder som kan användas för att skydda sig mot dessa attacker och hur väl dessa metoder fungerar. Resultaten består av en tabell som listar ut attackernas namn, beteende, försvarsstrategi, farans omfattning samt försvarsnivå. Farans omfattning är baserat på hur mycket en enhet eller ett nätverk påverkas av attacken och försvarsnivån visar hur svårt det är att implementera de säkerhetsåtgärder som tagits upp.

Jag tycker resultaten jag nådde besvarar de frågor jag ställde i början av arbetet. Några frågor som ”Vad är P2P?” och ”Vad är P2P säkerhet?” skulle ha kunnat ha ett lite längre och djupare svar. De källorna jag hade om P2P attackerna och hur man skyddar sig mot dem tog ganska långt upp samma saker, skulle kanske ha varit bra med andra källor som skulle ha sett på sakerna från en annan synvinkel.

KÄLLOR

Jaideep, Gera och Bhanu Prakash Battula. 2016, Survey on the Present State-of-the-Art of P2P Networks, Their Security Issues and Counter Measures. *International Journal of Applied Engineering Research 11.1 (2016): 616-620.* Tillgänglig: http://www.ripublication.com/ijaer16/ijaerv11n1_91.pdf

Friedman, Allan, och L. Jean. Camp. 2005, Peer-to-peer security. *The Handbook of Information Security. J. Wiley&Sons*. Tillgänglig: http://allan.friedmans.org/papers/P2Psecurity.pdf

Wang, Lin. 2006, Attacks against peer-to-peer networks and countermeasures." *T-110.5290 Seminar on Network Security.* Tillgänglig: http://www.tml.tkk.fi/Publications/C/22/papers/Wang_final.pdf

Yang, Yu, och Lan Yang. 2012, A survey of peer-to-peer attacks and counter attacks. *Proceedings of the International Conference on Security and Management (SAM).*

The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp). Tillgänglig: http://worldcomp-proceedings.com/proc/p2012/SAM9754.pdf

Vroonhoven, Jochem Van. 2006, Peer to peer security. *4th Twente Student Conference on IT, Enschede (January 30, 2006).* Tillgänglig: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.60.3334&rep=rep1&type=pdf

Oram, Andy. 2001, *Peer to Peer: Harnessing the power of Disruptive Technologies*, 448s. Tillgänglig: http://library.uniteddiversity.coop/REconomy_Resource_Pack/More_Inspirational_Videos_and_Useful_Info/Peer_to_Peer-Harnessing_the_Power_of_Disruptive_Technologies.pdf

Rubenking, Neil J. 2016, *The best free Antivirus protection of 2016.* Tillgänglig: http://uk.pcmag.com/antivirus-reviews/142/guide/the-best-free-antivirus-protection-of-2016 Hämtad: 5.12.2016

Quain , John R. 2016, *Do you really need to pay for antivirus software?* Tillgänglig: http://www.tomsguide.com/us/antivirus-software-pay-or-free,news-18570.html Hämtad: 5.12.2016

Criddle, Linda. u.å. *What is Anti-virus software?* Tillgänglig: https://www.webroot.com/in/en/home/resources/tips/pc-security/security-what-is-anti-virus-software Hämtad: 5.12.2016

Crawford, Douglas. 22.1.2016, *VPNs for beginners – What you need to know.* Tillgänglig: https://www.bestvpn.com/blog/38176/vpns-beginners-need-know/ Hämtad: 5.12.2016

Tarantola, Andrew 26.3.2013, *VPNs: What they do, how they work and why you're dumb for not using one.* Tillgänglig: http://gizmodo.com/5990192/vpns-what-they-do-how-they-work-and-why-youre-dumb-for-not-using-one Hämtad: 5.12.2016

Gordon, Whitson 27.1.2014, *A beginner's guide to encryption: what is it and how to set it up.* Tillgänglig: http://lifehacker.com/a-beginners-guide-to-encryption-what-it-is-and-how-to-1508196946 Hämtad: 5.12.2016