Examensarbete

Steganografi: Hur steganografi kan påverka nätverkssäkerhet

Steganography: How steganography can affect network security.

Examensarbete för kandidatexamen med huvudområdet Informationsteknologi

Grundnivå 22.5 högskolepoäng IT610G

Vårtermin 2021
2021-06-13

Student: Jonny Härö
c18jonha@student.his.se

Handledare: Dennis Modig
Examinator: Ali Padyab

Sammanfattning

Steganografi är en samling tekniker som kan användas för att dölja att informationsutbyte sker genom att bädda in information på ett sätt som gör det svårt att märka av dess existens. Dessa tekniker kan användas för goda ändamål så som att undvika censur och inskränkningar i yttrandefriheten, de kan också användas för skadliga ändamål som för kriminella/terrorist-organisationer att kommunicera obemärkt eller för att kringgå säkerhetsåtgärder på ett nätverk. Trender visar bland annat på att malwares i större utsträckning använder sig mer och mer av dessa typer av tekniker. Detta skapar problem för nätverkssäkerheten och i denna systematiska litteraturstudie så undersöks vilka problemområden dessa tekniker kan föra med sig för nätverkssäkerhet. Arbetet granskar tillgängliga vetenskapliga artiklar från två databaser som sedan analyseras för att identifiera återkommande problemområden. 30 artiklar gick vidare till analys där tematisk kodning användes och resultatet visar på fem stycken huvudområden som var och en för utmaningar med sig gentemot säkerhetsarbetet. Dessa områden är: Exfiltration av data från nätverk, infiltration av icke önskad data till nätverket, kommunikationskanaler för skadlig kod, svårigheter för tekniskt skydd att upptäcka och förhindra och försvårat utredande arbete. Arbetet visar bland annat på att skadlig kod kan ta nytta av dessa tekniker och att dessa tekniker kan vara kraftigt varierande i dess funktion. Vidare så diskuteras det hur dessa enskilda problemområden kan försvåra säkerhetsarbetet och ger förslag baserat på detta resultat om hur framtida forskning kan bedrivas.

Innehåll

1 Introduktion

Det är ett omfattande arbete för de inblandade att hålla säkerheten på ett nätverk god idag, den komplexiteten som finns och den stora variation på tjänster som många nätverk måste kunna leverera till sina användare gör att det i många nätverk finns många trafikflöden in och ut. Att ha en bred kunskap om de olika utmaningar som det kan föra med sig när det gäller nätverkssäkerhet är något som är viktigt och hålla sig uppdaterad om nya hot är en tidskrävande utmaning som är ständigt pågående. Något som är mer och mer förekommande vid cyberattacker idag är ämnet steganografi.

Steganografi är ett delområde till ”Information Hiding” som kan använda sig av en samling av tekniker för att dölja att informationsutbyte sker. Detta är ett område som kan användas av illasinnade för att kringgå bland annat de skydd som finns implementerade på nätverk. Trender visar på att av de malwares som blir identifierade så syns en ökning på malwares som använder sig utav informationsdöljande tekniker. Detta är något som tidigare endast hittades i mycket sofistikerade malwares men nu observeras i typiska varianter av dessa (Mazurczyk & Wendzel, 2017). Steganografi är ett brett område med många olika tekniker och vid bakgrundsforskning till detta arbete så märktes en avsaknad av övergripande forskning på vilka typer av hot dessa kan föra med sig sett ur perspektivet på nätverkssäkerhet.

Att sammanställa dessa problemområden kan ge en bra grund för framtida forskning och göra det enklare att få en överblick av området vid inledande forskning. Detta arbete identifierar problemområden via en litteraturstudie som sedan presenteras och diskuteras.

2 Bakgrund

Steganografi är en samling av tekniker som har som mål att bädda in information i bärare i ett syfte för att gömma den, det kan ställas i kontrast till kryptografi som handlar om att det finns ett meddelande som inte är dolt men dess innehåll är det, medan steganografi syftar på att gömma meddelandets existens helt och hållet. Meddelandets innehåll behöver inte vara dolt men kan i kombination med kryptografi dölja dess innehåll. Detta har som effekt att meddelanden då kan ”smugglas” i kamouflerade former som annars skulle kunna väcka misstanke om dess existens. När informationen sedan nått sitt mål så kan parten eller parterna som är medvetna om den gömda datan extrahera den utan att någon märkt att det överhuvudtaget skickats dold information.

Orden kryptologi och steganografi båda härstammar ifrån grekiskan och löst översatt står ordet kryptologi står för ”hemlig skrift” medan steganografi står för ”dold skrift”, den ena metoden gömmer meddelandets innehåll medans den andra gömmer kommunikations-kanalen. (Zielinska, Mazurczyk, & Szczypiorski, 2014).

Ett exempel på ett legitimt sätt där teknik för att gömma data används idag är med

digitala vattenmärken, det kan vara exempelvis video-on-demand tjänster som bäddar in ett vattenmärke i filmen som en kund hyr. Om denna film sedan skulle dyka upp på piratsajter så kan vattenmärket extraheras för att se vilken kund som har distribuerat filmen olagligt. Vissa särskiljer dock vattenmärken från steganografi, båda tillhör kategorin ”Data-hiding” men i kontrast till vattenmärket som står i relation till dess bärare och denna bärare ofta är av värde så har steganografin oftast ingen relation med sin bärare och ser inte sin bärare som något värdefullt utan utnyttjas bara för att bädda in och transportera information. Dock kan dessa två kategorier överlappa varandra vid olika scenarion. (Megías, 2020).

2.1 Centrala koncept

I denna sektion så beskrivs de koncept som läsaren bör vara medveten om för att kunna ta till sig informationen i arbetet till fullo.

2.1.1 Bärare av dold information

Dessa bärare av dold information så kallade ”Carriers” och även kallat ”Covers” kan vara av varierade slag så som multimedia (bilder, videos, ljud mm.) och fysiska objekt men det går även att nyttja nätverks och kommunikations-protokoll som bärare (Megías, 2020).

Historiskt sett så har dessa bärare av information varierat kraftig och ständigt förnyats i takt med teknikens utveckling. Några av de tidigaste dokumenterade bärarna inom steganografin är meddelanden gömda i harar kamouflerade som jakttroféer från det antika Grekland. Även träplattor med graverad skrift dolt bakom ett vax-lager från denna tidsperiod nämns.

När papper började användas för skrift så användes även detta som bärare i kombination med osynligt bläck gjort på sav som kunde värmas för att göra det synligt. Detta utvecklades sedan vidare till att gömma information i vanlig skrift, andra fysiska objekt, musiknoter, mikroskopiska objekt, radiovågor med flera. Dessa bärare utvecklades sedan i takt med den digitaliserade tekniken (Zielinska, Mazurczyk, & Szczypiorski, 2014).

Modern steganografisk teknik kan ta nytta av dagens digitala teknik i form av datorer och nätverk. Detta kan påverka det säkerhetsarbetet som en nätverks eller systemadministratör utför, så som exempelvis se till att känslig information inte lämnar nätverk och även skydda nätverk från att få skadlig kod hämtat till sig.

Moderna bärare för steganografiska tekniker tar nytta av bland annat digital media, bilder har flera egenskaper som är lämpade för att bädda in information i, spatial information som värden av intensitet på pixlar och även filformatets varierande data-fält kan nyttjas.

Ljudfiler har också utrymme i deras olika egenskaper till att bära information så som att exempelvis utnyttja ”Spread spectrum” för att bädda in information i pseudo-slumpmässiga frekvenser över ljudfilens frekvensregister.

Video-filer som bärare ger ännu mera utrymme att bädda in information, där kan

exempelvis tekniker från både ljud och bild-steganografi kombineras.

Nätverks-steganografi är synonymt med ”Covert channels”, det vill säga att dessa metoder används för att skapa ”dolda kanaler” som information kan strömma in eller ut igenom. Dessa kan ta nytta av de olika protokollen som finns på de olika lagren i OSI-modellen för att bädda in information.

Som synes så är det flera olika metoder eller typer av steganografiska bärare som kan användas för att angripa nätverk av illasinnade, de kan användas var för sig eller kombineras för att ytterligare försvåra dess upptäckt eller göra det enklare för angripare att extrahera, skicka in data eller styra malwares i nätverk som de har fått ett fäste i. I artikeln ”Trends in Steganograhpy” (Zielinska, Mazurczyk, & Szczypiorski, 2014) så ger författarna en överblick över de olika steganografiska metoderna som finns till förfogande för att bädda in information och dölja dess existens. Författarna nämner fyra huvudområden där modern digital steganografisk teknik kan delas upp:

- Digital media-steganografi

  Syftar till att bädda in information i media så som bilder, video, ljud och liknade format.

- Språklig/text (Linguistic)-steganografi

  En teknik där information bäddas in i läsbar text och endast de som vet vilka delar av meddelandet som egentligen innehåller dold information kan läsa ur det.

- Filsystemssteganografi

  En metod att utnyttja mekanismer i filsystem för att dölja information, exempelvis skriva data till ett område i en hårddisk och få det till att se ut som slumpmässiga bits.

- Nätverkssteganografi

  Utnyttjande av protokoll för att dölja data, exempelvis genom att ta nytta av naturliga störningar som vanligtvis sker, utnyttja redundant information som protokollet för med sig eller att använda sig av friheter för egen implementation som protokollet tillåter. Detta helst genom att undvika att störa det underliggande protokollets funktion för att ej sticka ut som en anomalitet eller dra uppmärksamhet till sig.

Dessa kan var för sig eller i kombination med varandra påverka säkerheten på ett nätverk som synes i exemplet med attacken ”Sunburst” som nämns senare i arbetet. Som nämnts ovan så finns det flera olika möjligheter att bädda in data i bärare av varierande slag, att undersöka dessa för att se om det finns dolda meddelanden eller för att försöka läsa av den dolda informationen så används metodiken ”Steganalysis”, på svenska ”Stegoanalys” [egen översättning].

2.1.2 Stegoanalys

Precis som inom kryptologin så som kryptografi har kryptoanalys för att dechiffrera dess innehåll så kallas steganografins motsvarighet för stegoanalys (Engelska: ”steganalysis”) vars syfte är att finna dolda meddelanden.

De verktyg som används för modern staganalysis delas vanligvis upp i två olika huvudkategorier för att kunna analysera, upptäcka och extrahera dold information:

- Blind attack
- Riktad attack

Vid blinda attacker så utgås det från att analytikern inte har någon kännedom alls om ifall det överhuvudtaget finns dold data och inte heller om vilka metoder som kan ha används. Denna typ av undersökning är mycket mer krävande än riktade attacker men kan anses mer modern och kraftfull just på grund av att dessa metoder inte är låsta till specifika inbäddningsmetoder. Exempel här skulle kunna vara stickprover på olika typer av potentiella bärare.

Riktade attacker är när analys görs i kombination med en idé om att upptäcka en viss typ av steganografisk process eller tillvägagångsätt. Dessa typer av undersökningar lämpar sig då när misstanke finns kring att steganografiska tekniker har använts (Douglas, Bailey, Leeney, & Curran, 2017). Exempel här kan vara om det påträffas mjukvara för att bädda in information i bilder på en anställds dator så kan riktade attacker användas för att söka igenom de bilder som finns lokalt för att undersöka om denne försökt läcka information och förhoppningsvis även se vilken information.

Dessa två kategorier av analysmetoder har sedan flera olika metoder och tillvägagångsätt till sitt förfogande, vidare så hävdar Megías (2020) också att system-attacker också är ytterligare en kategori. Denna kategori syftar på att utnyttja svagheter i implementationen från det valda steganografiska verktyget som använts för att bädda in information. Värt att nämna är att under detta arbetets gång så gavs intrycket att mycket att den tidigare forskningen kring stegoanalys verkar vara fokuserat på analys av bilder (digital media-steganografi). Ker et al. (2013) forskar djupare på stegoanalys just för nätverkssteganografi och diskuterar bland annat om att lärdommar kan tas från stegoanalys metoder från andra områden.

2.2 Bakgrund till relaterat område

I denna del så beskrivs tidigare forskning kring området och ger en inblick till vad arbetet kommer handla om.

2.2.1 Steganografi som ett hot mot ett nätverks säkerhet

Användandet av steganografiska tekniker inom bland annat malwares gör att det är svårt att upptäcka dess kommunikations-kanaler med exempelvis ”Command & Control”-servrar när data exfiltreras ut från ett nätverk eller när skadlig kod hämtar instruktioner från en sådan server. Illasinnade angripare bäddar helt enkelt in information i bärare så som bilder, videos, ljud, text eller protokoll och när dessa sedan passerar in och ut genom nätverk så finns det oftast ingen anledning till att implementerade säkerhetslösningar skulle höja några larm. Detta är en trend som har visat sig inte bara användas vid cyberspionage operationer utan även något som cyber-kriminella har anammat i uppdaterade versioner av trojaner, något som leder till förhöjd komplexitet när det gäller att finna dessa malwares (Kaspersky, 2017).

Dessa typer av skadlig kod kallas ibland ”Stegware” eller ”Stegomalware”.

För att ytterligare understryka hur pass svårt arbetet är med säkerhet när steganografiska tekniker används så är det bara att se på en av de senaste mer allvarliga cyberattackerna som rapporterades i december 2020 om Solarwinds Orion-plattform som fått smeknamnet ”Sunburst”. En attack som beskrivs som en av de mest allvarliga i modern tid som påverkade över 18 000 kunder till Solarwind. Kunder som bland annat innefattar flertalet departement i USA så som Pentagon, Department of Homeland Security, Department of Energy, National Nuclear Security Administration och amerikanska finansministeriet. Även privata bolag så som Microsoft, Cisco, Intel med flera attackerades, utredning pågår fortfarande under skapandet av detta arbete för att se över skadorna men man vet att flertalet mejl konton och nätverk har blivit äventyrade (Jibilian & Canales, 2021).

I denna attack så har angripare hackat Solarwind och skickat med en trojan i en uppdatering till deras plattform Orion. Denna trojan använde sedan steganografiska tekniker för att upprätta så kallade ”covert-channels” med hjälp av DNS-uppslag som bärare. DNS-uppslag gjordes mot en av angriparnas servrar och svaret var IP-adresser som egentligen berättade för trojanen hur den skall agera. Något som gjorde det svårt att upptäcka va att det var helt vanliga IP-adresser men beroende på inom vilket spann adressen befann sig så skulle trojanen agera olika på detta. När angriparna fick intresse för något så kunde de gå vidare till ytterligare en fas där steganografisk teknik bäddade in information till HTTP-GET förfrågningar och hämtade sedan en XML fil som också agerade som bärare och hade ytterligare instruktioner inbäddade (Symantec Threat Hunter Team, 2021)

Detta är bara ett av många exempel av malwares som använder sig av steganografiska tekniker för att utföra det de är designade till på ett sätt som gör dem svåra att upptäcka. I takt med de framsteg som sker för att göra system säkra så tvingas skaparna av dessa malwares till mer sofistikerade metoder för att kringgå

den hårdare säkerheten och avancerade verktygen som finns för att upptäcka deras kod eller metoder. En av de större tidigare incidenterna där steganografiska tekniker användes på stor skala kan spåras tillbaka till 2006 med attacken ”Operation Shady RAT” som hade angripit flertalet internationella mål och ställde till med skada i flera månader. Här laddade viruset ”Trojan.Downbot” ner filer som HTML-sidor och JPEG bilder som agerade som steganografiska bärare där informationen som var inbäddad var kommandon för att kommunicera med den skadliga koden. Sedan dess så har det kontinuerligt dykt upp nya malwares med informations-döljande egenskaper (Mazurczyk & Caviglione, 2015).

Författarna Mazurczyk & Caviglione (2015) diskuterar om de svårigheter som upptäckandet av malwares av denna typ för med sig. De kartlägger några av de mest populära typerna av skadlig kod som har steganografiska egenskaper som dykt upp mellan 2011 och 2014. De inkluderar även ”proof-of-concept”-malwares som förts fram av forskarvärlden. Sammanställningen visar på att de åtgärder som tas av den skadliga koden för att dölja dess existens är kraftigt varierande i funktion och deras process kan kraftigt skilja sig åt från andra malwares av denna typ. Denna variation kan göra att tillvägagångsättet för att kunna upptäcka dem skiljer sig åt så pass att det är svårt att kunna införa förebyggande skydd och även upptäcka att ett nätverk i stunden är angripet.

I artikeln ” The New Threats of Information Hiding: The Road Ahead” (Cabaj, Caviglione, Mazurczyk, Wendzel, Woodward, & Zander, 2018) så ger författarna en överblick av olika malwares och de tekniker som dessa använder sig av för att gömma information. De diskuterar även de hot som existerar och är på uppgång och menar på att den rollen som ”information-hiding” har fått inom skadlig kod i dagsläget är erkänd och att det med största sannolikhet kommer ha en ännu mer betydande roll i framtiden. De menar också på att de tidigare metoderna med att använda sig av digital media som bärare har evolverats vidare till att istället använda nätverks-steganografi för att de för med sig fördelar så som att en kontinuerlig ström av data kan upprätthållas genom en så kallad ”covert-channel” för att exempelvis långsamt läcka ut information genom brandväggar i trafik-typer som ej filtreras av denna. De påpekar också att dessa metoder för att gömma data har gått från att vara enbart implementerat i de mest sofistikerade typerna av nationellt sponsrad skadlig kod till att bli en standard för vanliga typer av malwares.

Vidare så vill även författarna skilja på vad som är klassat som steganografi och obfuskering, där steganografi försöker kommunicera på ett sätt som ej går att se medans obfuskerad kommunikation kan vara helt synlig men dess innebörd eller syfte är svårt att förstå.

2.2.2 Tidigare relaterad forskning

Författarna Zielinska, Mazurczyk, & Szczypiorski (2014) ger en bra överblick över vad steganografi är, hur det använts historiskt och vilka trender som syns. De diskuterar malwares som använder sig av dessa typer av tekniker och även andra sätt så som digital media steganografi och nämner kort hur dessa har använts tidigare för att exempelvis smuggla data ur ett nätverk. De nämner också hur dessa tekniker ofta kan passera genom nätverk utan att sticka ut som anomaliteter ihop

med att nätverkens komplexitet ger många möjligheter att använda steganografi på illasinnade sätt.

Mazurczyk & Wendzel (2017) nämner kort hur informationsdöljande tekniker kan användas av cyberkriminella för ändamål så som exfiltrering av konfidentiell information och hur det även kan användas för kommunikationskanaler för skadlig kod. De diskuterar även de svårigheter som finns med att upptäcka att ett system är utsatt för en attack som involverar steganografi. Fokus på artikeln ligger dock mest på det är en utmaning att hantera dessa tekniker ur ett forensiskt perspektiv men en del är ändå relevant för nätverkssäkerhet så som exempelvis vid en incident-analys vid en attack kunna utreda internt vad som har hänt, vilka metoder angripare har använt sig av, vilken information som har ändrats/läckt/infiltrerats eller på annat sätt påverkats för att kunna sätta in åtgärder.

Vidare så diskuterar Lubacz, Mazurczyk, & Szczypiorski (2014) nätverks-steganografi och ger en bra överblick hur de olika lagren på OSI-modellen och dess protokoll som kan utnyttjas som bärare, de uttrycker också att det är en avsaknad av systematiska diskussioner utav principerna och teknikerna kring nätverks-steganografi. De diskuterar även hur skiftet från de traditionella kretskopplade (circuit switched) nätverken där tjänsterna är försedda av nätverket så som transport och kontroll funktionerna till dagens paketförmedlade (packet switched) nätverk har lett till att nätverks-steganografi har kunnat växa fram. Här är inte längre transport och kontrollfunktioner separerade, utan här är de nu mottagliga för påverkan utav användare.

3 Problem och forskningsfråga

Detta kapitel beskriver och motiverar forskningens mål och motiverar vad det kan bidra med till arbetet för att hålla säkerheten på ett nätverk god och även vad det kan bidra med till för vidare forskning inom området. I följande underkapitel beskrivs också arbetets avgränsningar.

3.1 Forskningsfråga

Frågeställningen som skall besvaras är:

”Vilken påverkan kan steganografi ha på nätverkssäkerhet?”

3.2 Motivering

Dagens komplexitet när det gäller de många olika protokollen som används inom nätverks-kommunikation gör att det finns många möjligheter att utnyttja dessa som steganografiska bärare på ett sätt som göra att det är svårt att identifiera och upptäcka. Det är en stor variation av data som kommer in och ut till nätverken och många av de olika data-fälten i protokollen lämnar de sårbara för att bädda in information så som exempelvis i funktioner inom protokollen för att hantera fel, fördröjningar, fragmentering och likande. De protokollen som kan användas i sådant syfte behöver inte heller vara från specifika delar av OSI-modellen utan alla lager kan utnyttjas för manipulation av dess data (Lubacz, Mazurczyk, &

Szczypiorski, 2014).

Det är viktigt att dessa möjligheter belyses för att kunna sätta in åtgärder och vara medveten om riskerna som finns. Att även fortsätta belysa detta i framtiden kan förhoppningsvis leda till att det tas i beaktning av design av nya protokoll och vid uppdateringar till befintliga protokoll.

Vidare så växer ständigt cyberbrottslighet på grund av flertalet faktorer så som att uppkopplade internetanvändare ständigt ökar, uppkopplade enheter blir fler, komplexiteten på och mängden av olika protokoll ökar ihop med att fler och fler tjänster blir digitaliserade. Detta leder till att många nya malwares utvecklas i en snabb takt och tar nytta av dessa faktorer för att göra skada. Under 2019 så hade det av Kaspersky identifierats en ökning på 14 % av nya, unika, skadliga objekt jämfört med året innan (Caviglione, o.a., 2020).

Enligt Cabaj et al. (2018) så anses egenskaper och tekniker för att dölja information vara en av de huvudsakliga nya trenderna inom cyberbrottslighet, förövarnas vilja att förbli oupptäckta och att försvåra spårning av ursprunget till malwares anses vara den huvudsakliga motivationen till detta och därför kommer cyberkriminella ständigt försöka förbättra sina tekniker på detta område. Författarna menar också på att de steganografiska teknikerna som används idag oftast inte ens behöver hög grad av komplexitet på grund av att de skyddssystem som används idag så som exempelvis ”Intrusion Detection Systems” i praktiken har väldigt svårt att upptäcka steganografiska bärare. Vidare så anser de att moderna malwares har blivit så effektiva att de kan ligga dolda under långa perioder och även om inte steganografi är den huvudsakliga orsaken till svårigheterna att upptäcka dem så har det definitivt en roll i svårigheterna att upptäcka och bekämpa dessa. Författarna uttrycker också att det finns en oroväckande avsaknad av tekniker för att upptäcka hot som använder sig av metoder för att gömma information.

Mycket om forskningen inom detta område verkar handla om idéer för hur steganografi kan implementeras, hur skydd kan utvecklas, summeringar av de olika typerna av bärare, dess metoder och hur de kan användas. Det diskuteras inte så mycket om hur dessa tekniker övergripande ur ett perspektiv från nätverkssäkerhet försvårar säkerhetsarbetet och vilka hot och utmaningar det för med sig.

3.3 Forskningsmål

Målet med detta arbete är att på ett strukturerat sätt sammanställa de utmaningarna och hoten steganografi kan ställa mot att hålla säkerheten på ett nätverk god. Att belysa tidigare incidenter och trender som denna samling av tekniker används till för att försvaga säkerheten eller kompromissa säkerheten på ett nätverk. Detta görs för att höja medvetenheten om denna typ av hot som ständigt utvecklas och förnyas i ett syfte för att kunna forska vidare om åtgärder som kan tas för att minska dess negativa påverkan eller för att kunna planera för att sätta in skydd. Steganografin verkar inte få så mycket uppmärksamhet som den egentligen förtjänar sett till hur pass stor utmaning den för med sig för nuvarande och framtida säkerhetsarbete kring nätverk.

Att identifiera de problemområden som illasinnad användning av steganografiska tekniker för med sig för nätverkssäkerhet på ett systematiskt sätt leder till att vidare

forskning inom dessa problemområden får en grund att jobba vidare från. Mycket av forskingen inom området verkar inte fokusera på att sammanställa hur de olika steganografiska teknikerna påverkar eller kringgår nätverkssäkerhet. Det finns mycket sammanställande forskning kring hur de olika teknikerna kan användas och upptäckas men ett fokus på dessa tekniker från övergripande perspektiv av nätverkssäkerhet kan göra att det blir enklare att ge sig in i området och sedan specificera in sig vidare på något av de identifierade problemområdena.

Förhoppningen är att lärdomar kan tas av tidigare incidenter och belysning av problemområden för att kunna upptäcka liknande attacker idag och även att informationen kan tas i beaktning i design av skydd för framtida hot av liknande natur. Dessa lärdomar kan exempelvis vara tidigare tillvägagångsätt och en förståelse för varför de tekniska skydden inte räckte till för att skydda nätverken.

3.4 Avgränsningar

Detta arbete kommer ha som mål att ge en strukturerad sammanfattning av de hot som steganografin kan ställa mot ett nätverks säkerhet. Arbetet kommer därför inte ta med åtgärder som kan tas för ökat skydd eller några rekommendationer. Vidare kommer de tekniker som används för skydd i dag inte diskuteras på djupet heller. De tekniska detaljerna på de olika identifierade problemområdena kommer diskuteras på en övergripande nivå med syftet att få en bred övergripande grund.

4 Metod

Denna del av rapporten kommer beskriva den metod som används för denna studie.

För att kunna svara på forskningsfrågan så kommer arbetet bestå av en litteraturstudie där artiklar med relevans läses igenom och återkommande teman som påvisar de hot som ställs gentemot nätverkssäkerheten identifieras, sammanställas och presenteras.

Valet av metod för detta arbete är systematisk litteraturstudie, tidigare arbete av Templier & Paré (2015) visar på att en litteraturstudie är viktigt för att belysa tidigare studier och forskning inom ett ämne, litteraturstudier erbjuder grunder för fortsatta vetenskapliga forskningar och är grundläggande för ett vetenskapligt områdes vidare utveckling.

4.1 Litteraturstudie

I denna sektion beskrivs det hur litteraturstudien i detta arbete går till, de databaser som används och de sökord som är aktuella. De insamlade artiklarna matchas sedan mot fördefinierade kriterier som avgör om de ska inkluderas eller exkluderas. Sedan beskrivs hur den insamlade datan analyseras.

4.1.1 Förklaring av metod

Enligt Templier & Paré (2015) så är det sex steg som ska genomföras vid en litteraturstudie:

1. ”Formulating the problem”
2. ”Searching the literature”
3. ”Screening for inclusion”
4. ”Assessing quality”
5. ”Extracting data”
6. ”Analyzing and synthesizing data”

Steg ett är då först att formulera problemet, det innebär att det ska definieras vad målet med litteraturstudien är, detta ihop med förklaring om centrala begrepp och motivering om varför litteraturstudien är nödvändig. Detta gjordes här i kapitel tre.

Steg två är sedan att genomföra sökning i tillgänglig litteratur, detta är början på data insamlings-fasen. Här så skall informationskällor hittas och studier som är relevanta till arbetet.

I steg tre så ska den insamlade datan evalueras för att se om materialet går att applicera till litteraturstudien och om de ska inkluderas eller exkluderas. Detta görs i det här arbetet med fördefinierade exkluderingskriterier och ett beskrivet tillvägagångsätt för att avgöra dess relevans.

Nästa steg är att avgöra kvalitén på den insamlade datan, detta görs här genom att dels enbart inkludera granskat och publicerat material ihop med att läsa artiklarna själv.

Steg fem är samla information från de insamlade artiklarna som är applicerbara på arbetet. Detta görs här genom att läsa igenom artiklarna och markera de stycken som är relevanta till litteraturstudien.

Sista steget är att analysera datan, detta genom att organisera, jämföra, kollationera, summera, aggregera eller tolka informationen som samlades in för att kunna föreslå bidragande av kunskap som litteraturstudien ger. Detta görs här med tematisk kodning.

4.1.2 Hur genomföra metod

För att samla in artiklar så kommer databaserna IEEExplore och ACM Digital Library att användas för litteraturstudien, detta på grund av att de mesta artiklarna är peer-reviewade och för att databaserna har ett gott utbud av material som bör vara tillräckligt för att svara på forskningsfrågan. Sedan kommer stegen som nämndes ovan att följas.

Databaserna kommer att genomsökas med följande söksträng:

Steganography AND ("covert channel" OR malware OR malicious)*

4.1.3 Avgränsningar i metod

För att se till att de artiklarna som används i arbetet har relevans och värde att bidra med till rapporten så användes följande exkluderings-kriterier för att sålla bort de som inte är av intresse:

- Ej kvalitetsgranskat material (Peer-reviewed conference papers eller journals)
- Artikel äldre än 10 år, detta för att undvika äldre problemområden som kan ha blivit åtgärdade och för att fokusera på den aktuella forskningen inom området.
- Inte skriven på svenska eller engelska
- Låg relevans till forskningsfråga (Avgörs genom att läsa abstract sen vidare till introduktion)

Vidare så kommer insamlande av artiklar avslutas när 30 artiklar av god kvalité och relevans sållats fram för att användas i arbetet, detta på grund av att litteraturstudien ska kunna utföras efter given tidsram. Av samma anledning så är detta arbetet begränsat till endast två databaser.

4.1.4 Hur analysera resultat av metod

När artiklar är insamlade och de har gått igenom processen med att bli jämförda med exkluderingskriterierna så analyseras de sedan med hjälp av analysmetoden tematisk kodning. Detta görs för att kunna sortera, hitta och lyfta fram information som är relevant till arbetet. Tillvägagångsättet är att artiklarna läses igenom, information som är av relevans markeras, sedan så analyseras och organiseras informationen av värde i teman som är av intresse för forskningsfrågan.

Nedan följer exempel på tillvägagångsättet för tematisk kodning detta arbete:

Relevant stycke från artikel	Identifierat (återkommande) tema	Organiserad och presenterad information
..of such mechanisms are network covert channels (CCs) which utilize subtle modifications to the legitimate network traffic to carry secret data. *Unfortunately, nowadays no general detection approach exists that is able to fight covert communication in an efficient and scalable manner. On the*	Svårigheter för tekniskt skydd att upptäcka och förhindra	Det finns i dagsläget inget skydd som är effektivt och skalbart för att kunna skydda eller upptäcka en bred variation av steganografiska tekniker eller ”covert channels”. Snarare så behövs för varje enskild steganografisk teknik implementeras ett skydd för just den specifika metoden….

contrary, typically for a given information hiding technique a dedicated detection solution is devised. That is why..		(Nowakowski, Zórawski, Cabaj, & Mazurczyk, 2020).
..attacks are becoming ever more complex and stealthy*, in order to elude well-known detection techniques based on signatures and behavioral patterns. As a paradigmatic example, steganography can be used to hide the presence of malicious code in digital media and network traffic is used as the carrier to covertly exfiltrate data or to stealthily orchestrate nodes of a botnet*. Therefore, many recent attacks are difficult to detect and such..	Kommunikationskanaler för skadlig kod	Malware behöver bli mer och mer sofistikerade för att undvika att bli upptäckta av effektivare skydd som utvecklas med tiden. Malware kan då ta till steganografiska tekniker för att kunna exfiltrera data, kommunicera med en ”Command and Control”-server ...(Carrega, Caviglione, Repetto, & Zuppelli, 2020).

4.1.5 Validitet av metod

Validiteten av resultatet påverkas till en viss grad på grund av partiskheten att använda enbart de databaserna som nämns ovan, även partiskheten att sålla bort artiklar på grund av dess relevans som är ett manuellt arbete påverkas av vad som själv anses vara relevant eller icke relevant. Även de exkluderingskriterier som tagits fram kan påverka validiteten av resultatet till viss del.

5 Genomförande av metod

Detta kapitel beskriver hur genomförandet av litteraturstudien gick till, det börjar med sökningar i databaserna för att sedan gå igenom processen för exkludering och inkludering, tillvägagångsättet för att avgöra kvalité och relevans, hur informationen från artiklarna samlades in, analyserades och summerades.

Sökträng	Träffar IEEExplore	Träffar ACM Digital Library
Steganography AND ("covert channel*" OR malware OR malicious)	171	288
Totalt antal träffar: 459st		

Exkluderingskriterier:	Förkortning:
Artikel äldre än 10 år	EX1
Ej kvalitetsgranskat material (Peer-reviewed conference papers eller journals)	EX2
Låg relevans till forskningsfråga (Avgörs genom att läsa abstract sen vidare till introduktion)	EX3
Inte skriven på svenska eller engelska	EX4

Applicerade exkluderingskriterier:	IEEExplore Efter exkludering:	ACM Digital Library Efter exkludering:
Inga	171	288
EX1	134	199
+EX2	131	187
+EX3	38	20
+EX4	38	20
Artiklar kvar efter exkluderingsprocess: 58st		

Utav dessa 58 artiklar så skall 30 artiklar av god relevans och kvalité väljas till att användas i arbetet och det görs genom att läsa igenom artiklarna i sin helhet för att avgöra om de är av värde för arbetet. De artiklar som är av mest värde för arbetet utav detta urval väljs sedan till att användas i analys-fasen. De artiklar som gick vidare till nästa fas presenteras i Bilaga A.

5.1 Hur metoden faktiskt genomfördes

För att få fram relevant data från artiklarna så lästes alla dessa igenom och text av värde för rapporten markerades. De stycken som är av värde till arbetet delades upp i teman som var återkommande bland forskningsartiklarna som lästes. Dessa återkommande teman presenteras i Appendix B – Konceptmatris ihop med artiklarnas relevans till dessa.

5.2 Resultat

Detta kapitel presenterar den insamlade informationen som hämtades från litteraturstudien, här är informationen samlad i teman som var och en visar på problemområden som dessa typer av tekniker för med sig i säkerhetsarbetet på nätverk. Här samanställs de svårigheter och utmaningar som måste hanteras för att kunna motverka de problem steganografiska tekniker för med sig om de används på ett illasinnat sätt.

5.2.1 Exfiltration av data från nätverket

Ett av hoten som steganografiska tekniker för med sig gentemot nätverkssäkerhet är att de kan användas för att exfiltrera data ut från nätverk på sätt som bryter mot policys och implementerade säkerhetsåtgärder.

Det kan till exempel vara företagshemligheter eller känsliga uppgifter som kan leda till stora ekonomiska skador för företag och organisationer. Det kan ske på sätt som gör att det är svårt att uppmärksamma och sätta in åtgärder innan skadan är skedd. Exempel på metoder som använts av angripare är bland annat att läcka ut data från nätverk med hjälp av tjänster så som YouTube och Vimeo där videofiler användes som bärare (Francis-Christie & Lo, 2016) eller att bädda in data i bilder som skedde när en anställd exfiltrerade ut finansiell data från US Department of Justice (Mazurczyk & Caviglione, 2014). Även malware designade för att angripa och exfiltrera data från så kallade ”air-gapped networks” (nätverk som ej är kopplade till internet) har använt sig av tekniker för att gömma den datan de samlar in, så som viruset ”Fanny” som spreds genom USB-stickor och samlade in information från nätverken och använde sig av filsystemet FAT (File Allocation System) som bärare. Viruset bäddade in den insamlade datan i dolda partitioner i FAT strukturen för att dölja den insamlade informationen. På detta sätt kunde angriparna rekognosera på nätverk, tjänster och enheter som planerades att aldrig vara anslutna till internet (Carrara & Adams, 2016).

Författarna Aljamea, Iliopoulos & Samiruzzaman (2016) uttrycker också att det är väldigt lätt för någon utan en teknisk bakgrund att använda sig av de mjukvaror som finns tillgängliga för att kunna bädda in data i exempelvis bilder för att på ett illasinnat syfte smuggla ut data från nätverken. De väljer bäraren de vill använda, väljer informationen de vill bädda in och mjukvaran sköter sedan resten åt dom, på detta sätt så kan data smugglas ut av en anställd på en organisation obemärkt även om organisationen exempelvis skulle scanna de anställdas skickade mejl.

Exfiltration av data kan också ske genom malware som när de fått fäste i ett nätverk läcker ut information genom att bädda in den stulna datan i olika typer av bärare för

att sedan passera ut genom skyddssystemen obemärkt.

Att som administratör eller nätverkstekniker kunna sätta regler för utgående data och se till att de inte bryts är av stor vikt. Att även kunna övervaka vilken trafik som passerar ut genom nätverket för att upptäcka flöden av intresse via manuell övervakning eller av ett SIEM (Security Information and Event Management) system för att slå larm är viktigt. Om dessa system kringgås så kan information läcka ut från nätverk som kan åstadkomma stor skada för de inblandade. Att kunna kringgå de skydd som finns på nätverket på detta sätt är ett problem för nätverkssäkerheten.

5.2.2 Infiltration av icke önskad data till nätverket

På samma sätt som steganografiska tekniker kan användas för att smuggla ut data från nätverk så kan även dessa tekniker användas för att skicka in data till nätverk på sätt som gör att de inte blir upptäckta av de skyddssystem som finns implementerade för att förhindra detta. Det kan vara att exempelvis malware hämtar ytterligare moduler genom att ladda ned bilder som har inbäddad skadlig kod som malwaret sedan extraherar. Exempel på malwares av denna typ är ”Stegoloader” som efter att den fått fäste i ett system laddar ner PNG-bilder från en fördefinierad URL, dessa PNG-bilder är då bärare för körbar kod som extraheras och sedan byggs ihop av denna så kallade ”loader” (Bąk, Bieniasz, Krzemiński, & Szczypiorski, 2018). Även här gäller det att det är av stor vikt att de regler som finns för inkommande trafik till nätverken följs och att trafik kan övervakas för att upptäcka när oönskad data flödar in i nätverket. Att ej kunna se den trafik som flödar in till nätverken kan göra att skadlig kod kan få fäste och sprida sig i ett nätverk under lång tid innan det märks och åtgärder kan tas för att minska skadan.

5.2.3 Kommunikationskanaler för skadlig kod

Malware behöver bli mer och mer sofistikerade för att undivka att bli upptäckta av de effektivare skydd som utvecklas med tiden. Malware kan då ta till steganografiska tekniker för att kunna exfiltrera data, kommunicera med en ”Command and Control”-server eller hämta hem ytterligare moduler (Carrega, Caviglione, Repetto, & Zuppelli, 2020). Typerna av bärare kan skilja sig åt och kan bestå av exemeplvis multimedia-filer eller nätverksprotokoll för att skapa så kallade ”covert channels” där den skadliga koden då skapar kanaler där information kan flöda på ett sätt som bryter mot policys och regler medans det kringgår skydd och undviker uppmärksamhet.

Viruset ”Duqu” från 2011 ett av de tidigaste angreppen där steganografiska tekniker i malware användes. Viruset bäddade in data i JPEG-filer för att sedan skicka det vidare till angriparens server och för de som övervakade nätverket så fanns det inga anledningar till att väcka misstanke när en vanlig bild passerar ut genom nätverket. Flertalet virus har sedan dess använt sig av liknande tekniker. Exempel på virus som använt sig av nätverks-steganografi (”Covert Channels”) för att kommunicera på ett obemärkt sätt är viruset ”Morto” som upp upptäcktes samma år som ”Duqu” av Symantec där viruset istället använde sig utav protokollet DNS (Domain Name System) för att kommunicera med angriparnas servrar, ”Morto” anses vara det första viruset som upptäckts där nätverks-steganografiska tekniker använts.

Exempel på mer moderna virus med dessa egenskaper är ”Regin” där flertalet protokoll användes för att skapa kanaler, här använde sig viruset utav ICMP (Internet Control Message Protocol), HTTP (Hypertext Transfer Protocol) och TCP/UDP (Transmission Control Protocol/User Datagram Protocol) för att kunna kommunicera utan att sticka ut som anomaliteter i nätverkstrafiken (Bąk, Bieniasz, Krzemiński, & Szczypiorski, 2018).

När en angripare fått ett fäste i ett nätverk och upprättat så kallade ”covert channels” till den skadliga koden så kan angiparen då fjärrstyra vad den skadliga koden skall göra, det kan exempelvis vara att rekognosera nätverket, fortsätta sprida sig till andra enheter, hämta och exfiltera information, ladda ner ytterligare konfigurationer/instruktioner eller styras som en del i ett så kallat ”bot-net”. Kommunikationen med den skadliga koden kan ske genom att använda sig av open-source mjukvaror så som ”Invoke-PSImage” som används mer och mer av malware-utvecklare. Denna mjukvara bäddar in Powershell-komandon med steganografiska tekniker i bilder som bärare, den skadliga koden hämtar bilden, extraherar och sedan utför de inbäddade instruktionerna. Dessa typer av kommunikation är svåra för skyddssystem att upptäcka (Puchalski, Caviglione, Kozik, Marzecki, Krawczyk, & Choraś, 2020).

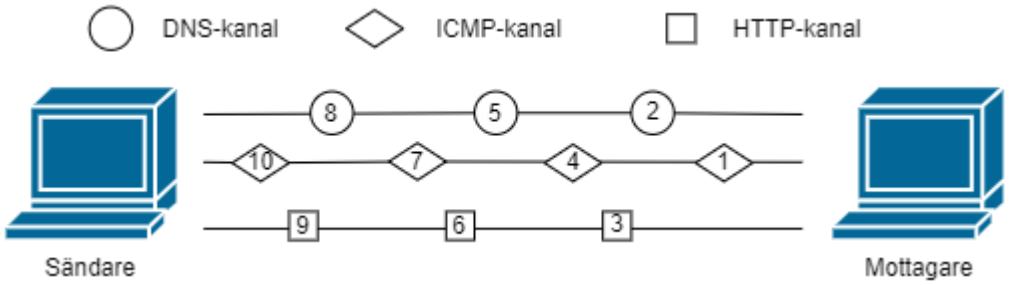
5.2.4 Svårigheter för tekniskt skydd att upptäcka och förhindra

På grund av den stora variationen av bärare så är det en stor utmaning att försöka förhindra att data passerar in och ut från nätverken på sätt som ej är tillåtna, att upptäcka att ett angrepp pågår i ett nätverk är också svårt.

De olika typerna av information som passerar in och ut från nätverk gör att det finns många olika sätt för angripare att dölja sin närvaro, bilder, video, ljud, text, nätverksprotokoll är typer av data som alla kan vara potentiella bärare av dold information (Chauhan, Jyotsna, Kumar, & Doegar, 2017). Det finns i dagsläget inget skydd som är effektivt och skalbart för att kunna skydda eller upptäcka en bred variation av steganografiska tekniker eller ”covert channels”. Snarare så behövs för varje enskild steganografisk teknik implementeras ett skydd för just den specifika metoden. Vidare så är mycket av forskningen fokuserad på stegoanalys av digital media som bärare så som bilder eller videos medan ett skifte nu pågår där mer och mer angripare vänder sig till att använda nätverks-steganografi (covert-channels) för att låta malware kunna skapa informationskanaler som är svåra att upptäcka (Nowakowski, Zórawski, Cabaj, & Mazurczyk, 2020).

Ytterligare metoder som angripare eller utvecklare av dessa malwares kan ta till sig är mer sofistikerade tillvägagångsätt så som ”Distributed Network Covert Channels”(DNCC) vilket i kontrast till vanliga covert channels som tillämpar ett flöde av information via en bärare så syftar DNCC till att sprida ut kommunikationsflödet parallellt över flera bärare eller tillämpa flera steganografiska metoder inom samma bärare. Det kan beskrivas som att det skapas flera covert-channels som kan användas på samtidigt eller användas turvis för att transportera informationen. Genom att sprida ut flödet på detta sätt så blir det inte så kraftiga förändringar i nätverkstrafiken kontra en covert-channel med samma bandbred som endast använder sig av en steganografisk teknik, det blir istället flera små förändringar istället för en stor. DNCC är något som fått mer uppmärksamhet inom

säkerhetsbranschen då dessa metoder skapar dolda kanaler som är svårare att upptäcka och kan kringgå vissa implementerade skydd på samtidigt som de tillåter en högre bandbredd (Cabaj, Mazurczyk, Nowakowski, & Żórawski, 2019).



Figur 1 - Exempel på paketflöden inom DNCC

Så kallade ”covert channels” komplexitet ökar ytterligare på grund av det finns två olika kategorier:

- Storage-channels
- Timing-channels

”Storage-channels” involverar direkt eller indirekt skrivande till ett lagringsutrymme av en process och ett direkt eller indirekt avläsande av detta lagringsutrymme av en annan process. ”Timing-channels” handlar istället om att tillåta en sändande process att signalera information till en annan genom att modulera sitt användande av systemresurser på ett sätt som påverkar den riktiga responstiden observerad av en annan process (Carrara & Adams, 2016). Exempel på ”storage-channel” kan vara att data lagras i eller modifieras i headern på ett nätverkspaket och exempel på ”Timing-channel” kan vara att variera tiderna på nätverkspaket för att på det sättet få fram ett meddelande till en mottagare. Något som kan vara värt att notera här är att i denna litteraturstudie så nämndes inga exempel på malwares som använt sig av ”Timing-channels” ute i det vilda ännu.

Forskare uttrycker svårigheter med att implementera skyddsåtgärder som kan upptäcka och förhindra en bred variation av steganografiska tekniker. Några gemensamma lösningar som återkommer i litteraturstudien är ofta baserade på noder kallade ”Wardens” (väktare) som kan vara placerade på olika platser i ett nätverk (Serrano Pérez, Rosales, & Cruz-Cortés, 2016). De kan ha en passiv roll där de undersöker trafiken efter anomaliteter eller en aktiv roll där trafiken modifieras. Det kan vara att trafiken ”saneras”, det vill säga att den trafik som passerar en aktiv warden modifieras så som exempelvis att redundanta fält i olika protokoll skrivs över i ett syfte att proaktivt försöka förstöra eller begränsa ett dolt informationsflöde (Szary, Mazurczyk, Wendzel, & Caviglione, 2020). Även maskininlärning är något som återkommer som en skyddsåtgärd i litteraturstudien men detta är utanför avgränsningarna i detta arbete.

För stegoanalys av nätverks eller digital media steganografi så finns det idag inget universellt skydd, varje stegoanalys-metod måste anpassas för den specifika steganografiska tekniken som används och de tekniker som finns idag är inte effektiva nog för att praktiskt implementera och övervaka trafik i realtid (Mazurczyk W. , 2013). Vidare så kan många forskare hålla med om att även om deras stegoanalys-verktyg kan fungera bra under laboratorieförhållanden så skulle deras noggrannhet vara opålitliga i faktiska implementationer, många studier gjorda skiljer sig från den verkliga miljön. Många forskare skulle hålla med om att de moderna verktyg som finns för stegoanalys idag ej skulle kunna användas effektivt i riktiga miljöer (Ker, o.a., 2013).

Den avsaknad av ett tekniskt skydd med bred effektivitet som uttrycks i flertalet artiklar leder till ett försvårat arbete för att sätta in åtgärder. Specifika metoder går att åtgärda men att täcka flera är tidskrävande och kan påverka prestandan på nätverket om trafiken ska analyseras på djupare nivå. Tekniska skydd så som brandväggar och IDPS (Instrusion Detection and Prevention Systems) är några av de viktigaste verktygen i arbetet med nätverkssäkerhet och en avsaknad av liknande system effektiva mot steganografi kan vara en svaghet i säkerhetsarbetet. Forskning görs på åtgärder genom att diskutera skydd med ett brett omfång av steganografiska tekniker men återkommande i denna litteraturstudie är att deras effektivitet ej ännu är tillräckliga.

5.2.5 Försvårat utredande arbete

Ytterligare ett problemområde som ej diskuterades så ofta men kan vara värt att belysa i litteraturstudien är det försvårade utredande arbetet när steganografiska tekniker använts. Utredande analyser kan behöva göras av polisväsende eller vid interna utredningar så som vid incidentanalyser vi ett cyberangrepp. Det kan vara av stor vikt att få reda på vilken information som exempelvis läckt ut vid ett cyberangrepp för att kunna vidta åtgärder för att minska ytterligare skada eller för att säkra det som bevis vid en eventuell rättegång.

Om målet för analytikern endast är att få konfirmation på att dold kommunikation har skett eller att hitta mål för vidare undersökning så är det möjligt att det kan ske utan full kännedom om den steganografiska metoden som använts för att bädda in informationen. Ker et al. (2013) menar på att en statistisk stegoanalys kan vara tillräcklig vid dessa tillfällen för att få det bekräftat. Vidare så menar författarna på att möjligheterna till att kunna extrahera och läsa av meddelandets innehåll kräver djupare kännedom om de inbäddningsalgoritmerna som använts. Att ta reda på vilken eller vilka algoritmer som använts kan vara svårt på grund av olika metoders snarlikheter.

En ytterligare svårhetet är de olika bärarnas livslängd, steganografi som involverar digital media som bärare som exempelvis en bild har kvar den inbäddade informationen för alltid, det gör att filen är mottaglig för analys och en möjlighet till att faktiskt lyckas extrahera den information som är dold där i. Här skapar dock nätverks-steganografi (”Covert channels”) utmaningar. I motsats till digital media steganografi så har inte vissa av dessa bärare en lång livslängd, det vill säga att efter dessa bärare har fyllt sin funktion så försvinner de, de lagras alltså inte och finns därför inte kvar för att kunna göra en analys på (Seo, Manoharan, & Mahanti, 2016).

Ett exempel är om data skulle vara inbäddad i ett redundant fält på ett TCP-paket så efter att paketet har skickats så finns det ingen kopia kvar av denna på systemet som den skickats från (vid exempelvis en exfiltrering). Exempel på varför det är av vikt att utreda vilken data som kan ha extraheras kan vara att identifiera att lösenordshashar har läckt och lösenord behövs bytas eller att känslig information kring kunder/personer/företag kan ha läckt och de måste bli underrättade om vad som läckt. Att inte kunna reda ut tillvägagångsätt eller vilken data som blivit påverkad gör att åtgärder ej kan sättas in för att förhindra att det sker igen eller förhindra ytterligare skada hos de påverkade.

6 Slutsats

Resultatet av denna litteraturstudie visar på att steganografiska tekniker kan ställa flera utmaningar på nätverkssäkerhetsarbetet. Dessa tekniker kan användas för flera ändamål av illasinnade för att kringå skydd och regler som finns implementerade för att styra dataflöde inom ett nätverk. I vissa fall så kan det även försvåra arbetet med att utreda vad som hänt vid ett angrepp i och med att visa bärare ej finns kvar för analys.

Både exfiltrering och infiltration av data ut och in till nätverk kan ske med olika typer av steganografiska tekniker och behöver inte enbart ske genom nätverkssteganografiska tekniker, även bärare så som videofiler, bilder, USB-minnen med dolda partitioner med mera kan användas för ändamålet. Exfiltrering av data från nätverk på ett sätt som kringår regler är ett problemområde för säkerheten på nätverk, detta kan leda till att känslig eller hemlig information läcker ut och kan orsaka skada. Att ej regler kan styra data som kommer in till ett nätverk är också ett problem, här kan exempelvis skadlig kod leta sig in till nätverken och orsaka skada.

Vidare så visar litteraturstudien på att malwares kan använda sig utav steganografiska tekniker för att skapa kommunikationskanaler där den skadliga koden kan både skicka och ta emot data till och från ett angripet nätverk. Dessa kanaler kan då bland annat användas för att fjärrstyra den skadliga koden via kommandon eller för att ladda hem ytterligare moduler. Att skadlig kod kan upprätta kommunikationskanaler genom metoder som är svåra att upptäcka kan göra att infekterade nätverk råkar ut för stora skador.

Litteraturstudien visar på att det är svårt att upptäcka och skydda nätverk från en bred variation av steganografiska bärare, ofta så måste för varje steganografisk teknik en specifik metod användas för att upptäcka och skydda mot denna. Artiklarna i studien visar på en avsaknad av ett skydd som kan täcka en bred variation av steganografiska bärare, något som försvårar arbetet med att skydda nätverket.

Utredning av vad som hänt eller vilken data som läckt ut ur eller skickats till ett nätverk vid en attack kan vara svårt när tekniker som dessa använts. Detta på grund av att vissa bärare ej finns kvar att kunna göra analyser på.

7 Diskussion

Denna delen av arbetet diskuterar metoden som utfördes, resultatet från litteraturstudien och hur den knyter sig till forskningsfrågan samt etiska och sammhälleliga aspekter. Metoddiskussionen diskuterar den egna studiens styrkor och svagheter som bland annat innebär kritisk reflektion av tillvägagångsättet. Resultatdiskussionen behandlar studiens resultat och vad detta arbete bidrar med för att svara på forkningsfrågan. Etiska och samhälleliga aspekter behandlar de etiska problem och eventuell samhällsnytta som arbetet för med sig.

7.1 Metoddiskussion

För att minska antalet irrelevanta träffar på sökningarna i databaserna så fick söksträngarna ändras för att minska omfånget, tidigare försök med söksträngar så som enbart ”steganography” eller i kombination med ”network security” ledde till ett omfång av ett högt antal artiklar som hade låg relevans. Att använda söksträngen ”Steganography” ihop med alternativen ”covert channels”, ”malware” och ”malicious” ledde till ett smalare resultat med bättre fokus gentemot arbetets mål. Fortfarande ledde sökningarna till många resultat som hade låg relevans så mycket av artiklarna fick läsas igenom för att avgöra om det var applicerbart på arbetet. Ändringarna gjorde dock att fokuset skiftades till illasinnad användning av steganografi på ett bättre sätt även om fokus från nätverkssäkerhets aspekten inte va fullt lika hög som förväntningarna var.

Det valet att smalna av sökningen till illasinnat bruk kan leda till att en del relevanta artiklar missas som hade kunnats fångas upp av att ha ett bredare omfång med mera träffar och istället manuellt läsa igenom fler av dessa. Valet att smala av sökningen motiveras dock med att arbetet ska kunna gå att genomföra inom given tidsram och att det är det illasinnade bruket av steganografi som kan påverka säkerheten som är av högst intresse för arbetet.

En svårighet med abetet var att många av de utvalda artiklarna inte diskuterar kring forskningsfrågan i större utsträckning, många artiklar nämner endast kortfattat hur de aktuella steganografiska teknikerna försvårar nätverssäkerhetsarbetet och hur de kan vara ett problem för säkerheten. Detta ledde till att många väldigt små stycken fick lyftas ut ur artiklarna för sedan att sammanställas ihop under det problemområde som det kategoriseras som. Informationsinsamlingen blev därför ganska ”spretig” men det ger också ett visst värde till detta arbete som nu gör det lättare att få en överblick över problemområdena på ett mindre tidskrävande sätt.

Antalet databaser som genomsöktes skulle kunnat utökas för att finna mer artiklar av värde, beslutet togs att enbart använda två stora databaser på grund av att dess utbud av artiklar är stora nog för att kunna uppfylla målet med arbetet.

En styrka i arbetet är att många exempel på attacker med skadlig kod som använt sig av steganografiska tekniker i riktiga angrepp presenteras i arbetet. Det går att ta lärdomar från hur dessa fungerar och varför vissa av dom har kunnat kommunicera obemärkta under längre perioder eller förstå varför de tekniska skydden inte hjälpte.

7.2 Resultatdiskussion

Resultaten från litteraturstudien visar på att steganografi har ett ganska brett användningsområde för illasinnat bruk. De identifierade problemområdena är inte många till antal men var och en ställer de utmaningar på säkerhetsarbetet. Dessa problemområden kan sedan brytas ner i mindre mer specifika områden då dessa är väldigt övergripande.

Bland artiklarna verkar det råda en viss oenighet om klassificering av olika tekniker, vissa författare så som Mazurczyk W. (2013) anser att ”covert channels” är en kategori tillhörande nätverks-steganogafi medans andra anser att det ska göras en åtskillnad, ett debatt som diskuteras djupare utav Jasolka & Khedri (2011). Dessa åtskilliga meningar om termer och klassificeringar kan ha gjort att vissa artiklar av relevans ej har blivit inkluderade i arbetet på grund av sökströngen som utgår från att ”covert channels” är en del av steganografi.

Ett problemområde som diskuterades mindre än väntat i litteraturstudien var det försvårade utredande arbetet. Det diskuterades inte så mycket bland artiklarna men det är ändå ett problemområde som är värt att ta upp och diskutera. Ett ämne som är närliggande detta är det försvårade forensiska arbetet som uppstår för utredare, något som diskuteras av Mazurczyk & Wendzel i artikeln ” Information hiding: Challenges for forensic experts” (2017).

Resultat som kan vara värt att lyfta fram i rapporten är problemområdet med kommunikations-kanaler för skadlig kod. Ett eget antagande är att det är från detta problemområde som de största utmaningarna ligger, som nämnt tidigare i arbetet så syns trender på att malwares med informationsdöljande tekniker kommer bli mer och mer vanligt. Åtgärder för att kunna upptäcka kanaler av dessa slag kan vara viktigt för framtida säkerhetsarbete och detta är ett område som troligtvis kommer behövas utvecklas i snabbare takt med tanke på utvecklingen och ökade användningen av malwares av dessa slag.

En artikel som går djupare och försöker kartlägga metoder för att åtgärda dolda kommunikationskanaler inom nätverksprotokoll är artikeln ” Network Protocol Covert Channels: Countermeasures Techniques” (Elsadig & Fadlalla, 2017). Här presenteras olika typer av ”covert channels” baserade på nätverksprotokoll, olika definitioner förklaras och sen lyfter artikeln även upp problemområden som är aktuella för dessa och diskuterar åtgärder. Bland annat så diskuteras trender så som ”micro-protocols”, ett protokoll som verkar inom den dolda kanalen för att göra en mer pålitlig dataström med exempelvis dynamisk routing.

Från den insamlade informationen går det göra några egna slutsatser baserat på detta arbete, komplexiteten på nätverkssteganografi kommer troligvis öka, detta baserat på den trend som syns med ökad användning av steganografiska tekniker samt utvecklingen av mer sofistikerade covert-channels så som ”Distributed Network Covert-channels”. Ytterligare en slutsats som går att göra är att tekniskt skydd troligtvis framöver kommer ha svårigheter att skydda nätverk och system från steganografiska tekniker baserat på dessa teknikers kraftigt varierande metoder och valmöjlighet av bärare samt att det uttrycks av forskare att tekniska skydd har svårt att upptäcka en stor bredd av dessa tekniker. Ett antagande är att det kan vara mer effektivt att uppdatera vissa befintliga protokoll för att slå ut dess användbarhet som

bärare samt begränsa vilka typer av potentiella bärare som får passera genom nätverken. Detta för att i ett proaktivt sätt slå ut möjligheterna för steganografiska bärare istället för att bara försöka identifiera upprättade eller försök till upprättande av kanaler. På detta sätt så kan även de tekniska skydden fokusera på att genomsöka ett färre antal av potentiella bärare, vilket kan leda till högre effektivitet.

Ytterligare en slutsats kan göras baserat på att flera olika malwares använder sig av liknande eller ibland samma bärare/protokoll för att kommunicera (exempelvis DNS-protokollet av ”Morto” och ”Sunburst”). Detta kan tyda på att även fast incidenter har skett med samma typ av steganografisk bärare så har inga eller för små åtgärder tagits för att skydda mot att det skulle kunna ske på samma sätt igen, det finns då en möjlighet att system och nätverk fortfarande nu är sårbara för precis samma tillvägagångsätt.

7.3 Etiska och samhälleliga aspekter

Resultatet av denna litteraturstudie pekar på områden där utmaningar och ibland fullgott skydd saknas när steganografiska tekniker används på ett sätt för att försöka kringå säkerhetsåtgärder inom nätverk. Resultatet kan därför inspirera och ge förslag till illasinnade som letar efter sätt att kringå skydd i nätverk, exempel ges på färdiga mjukvaror som kan bädda in information och kommandon i bärare för att ta sig förbi brandväggar och andra skydd. Även exempel på skadlig kod (malwares) beskrivs hur de har designats för att ta sig förbi skydd, något som utvecklare av skadlig kod kan imitera och implementera i eget skapande av skadlig kod. Dessa etiska problem får större effekt av att det uttrycks återkommande i materialet till litteraturstudien att det finns svårigheter att sätta in skydd som täcker en bred variation av steganografiska tekniker.

Samhällsnyttan av att belysa svårigheter och problem är dock viktig, att lyfta fram svårigheter gör att fler människor kan få intresse för att arbeta på lösningar så att vidare forskning inom området kan leda till faktiska skydd som i det här fallet påverkar många. Det ligger i intresset för alla som brukar datorer och nätverk att deras system eller information har ett tillförlitligt skydd och att forskningen fortsätter tillhandahålla skydd och åtgärder för de problem eller svårigheter som uppstår när nya typer av hot uppenbarar sig.

7.4 Framtida arbete

Framtida forskning inom området ”Svårigheter för tekniskt skydd att upptäcka och förhindra” skulle kunna vara av stort värde. Mer specifikt skydd för att upptäcka breda variationer av steganografiska bärare skulle göra stor nytta för området även om det kan vara en svår utmaning. Exempel på ett forskningsmål eller en riktning som kan underlätta vidare forskning skulle kunna vara ”Kartläggning av problemområden för tekniska skydd mot steganografiska tekniker”. I en sådan forskningsriktning så skulle de tekniska skyddens utmaningar kunna brytas ned till mindre delproblem som vidare forskning kan bedrivas på, exempelvis ”Hög resursåtgång/beräkningskraft för stegoanalys av bilder/etc. till och från nätverk” eller ”Fördröjning/latens som nackdel vid stegoanalys av inkommande/utgående

TCP/VoIP/DNS/etc.-trafik”.

Även en övergipande kartläggning av de steganografiska tekniker, val av bärare samt inbäddningsmetoder som har synts implementerade på riktiga malwares skulle vara av värde för att kunna kunna utveckla skydd mot steganografiska metoder som faktist är reella hot idag eller ta lärdom av vilka metoder som utvecklare av dessa ofta vänder sig till. Likande det arbete som Cabaj et al. (2018) gjorde i deras artikel ”The new threats of information hiding: The road ahead” och även Mazurczyk & Caviglione (2015) gjorde i artikeln “Information Hiding as a Challenge for Malware Detection” där den sistnämnda siktar på att gruppera malwares efter dess metoder för att dölja information.

Framtida forskning kan här kan även vara att bryta ner de övergripande identifierade områdena till mindre mer specifika delområden med ett bibehållet fokus på nätverkssäkerheten. Exempelvis:

- Exfiltration av data
    - Storage-channels
        - Metoder för att upptäcka
            - Network Wardens
                - Design och utvärdering av wardens
                - Experiment för att kunna kringå wardens
            - Machine learning
                - Experiment av maskininlärning med olika bärare
        - Metoder för att störa ut
            - Störa digitala media bärare
            - Störa nätverksprotokolls-bärare
            - Användning av aktiva network wardens
            - Utveckling av brandväggsregler för nätverksprotokolls redundanta data-fält
            - Forskning kring hur befintliga protokoll kan updateras för att slå ut dess användbarhet som steganografisk bärare
        - Kartläggning av storage-channels
            - Storage-channels påträffade i ”vilda” malwares
            - Kartläggning av potentiella steganografiska bärare

Referenser

Aljamea, M. M., Iliopoulos, C. S., & Samiruzzaman, M. (2016). Detection Of URL In Image Steganography. *ICC '16: Proceedings of the International Conference on Internet of things and Cloud Computing* (ss. 1-6). Cambridge United Kingdom: Association for Computing Machinery.

Bąk, P., Bieniasz, J., Krzemiński, M., & Szczypiorski, K. (2018). Application of Perfectly Undetectable Network Steganography Method for Malware Hidden Communication. *2018 4th International Conference on Frontiers of Signal Processing (ICFSP)*. Poitiers, France: IEEE.

Cabaj, K., Caviglione, L., Mazurczyk, W., Wendzel, S., Woodward, A., & Zander, S. (2018). The New Threats of Information Hiding: The Road Ahead. *IT Professional Volume: 20, Issue: 3*, 31-39.

Cabaj, K., Mazurczyk, W., Nowakowski, P., & Żórawski, P. (2019). Fine-tuning of Distributed Network Covert Channels Parameters and Their Impact on Undetectability. *ARES '19: Proceedings of the 14th International Conference on Availability, Reliability and Security* (ss. 1-8). Canterbury CA United Kingdom: Association for Computing Machinery.

Carrara, B., & Adams, C. (2016). A Survey and Taxonomy Aimed at the Detection and Measurement of Covert Channels. *IH&MMSec '16: Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security* (ss. 115-126). Vigo Galicia Spain: Association for Computing Machinery.

Carrega, A., Caviglione, L., Repetto, M., & Zuppelli, M. (2020). Programmable Data Gathering for Detecting Stegomalware. *2020 6th IEEE Conference on Network Softwarization (NetSoft)*. Ghent, Belgium: IEEE.

Caviglione, L., Choras, M., Corona, I., Janicki, A., Mazurczyk, W., Pawlicki, M., o.a. (2020). Tight Arms Race: Overview of Current Malware, Threats and Trends in Their Detection. *IEEE Access Volume 9*, 5371-5396.

Chauhan, S., Jyotsna, Kumar, J., & Doegar, A. (2017). Multiple layer text security using variable block size cryptography and image steganography. *2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT)*. Ghaziabad, India: IEEE.

Douglas, M., Bailey, K., Leeney, M., & Curran, K. (den 20 Januari 2017). An overview of steganography techniques applied to the protection of biometric data.

Elsadig, M. A., & Fadlalla, Y. A. (2017). Network Protocol Covert Channels: Countermeasures Techniques. *2017 9th IEEE-GCC Conference and Exhibition*. Manama, Bahrain: IEEE.

Francis-Christie, C., & Lo, D. (2016). A Combination of Active and Passive Video Steganalysis to Fight Sensitive Data Exfiltration through Online Video. *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*. Atlanta, GA, USA: IEEE.

Jasolka, J., & Khedri, R. (2011). Exploring Covert Channels. *Proceedings of the 44th Hawaii International Conference on System Sciences*. IEEE.

Jibilian, I., & Canales, K. (den 25 Februari 2021). *BusinessInsider.com*. Hämtat från Here's a simple explanation of how the massive SolarWinds hack happened and why it's such a big deal: https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12

Kaspersky. (den 03 Augusti 2017). *kaspersky.com*. Hämtat från Kaspersky Lab Identifies Worrying Trend in Hackers Using Steganography: https://usa.kaspersky.com/about/press-releases/2017_kaspersky-lab-identifies-worrying-trend-in-hackers-using-steganography

Kaspersky Lab. (den 11 Juni 2015). *Kaspersky Content Hub*. Hämtat från The Mystery of Duqu 2.0 a sophisticated cyberespionage actor returns: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07205202/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf

Ker, A. D., Bas, P., Böhme, R., Cogranne, R., Craver, S., Filler, T., o.a. (2013). Moving steganography and steganalysis from the laboratory into the real world. *IH&MMSec '13: Proceedings of the first ACM workshop on Information hiding and multimedia security* (ss. 45-58). Montpellier France: Association for Computing Machinery.

Lubacz, J., Mazurczyk, W., & Szczypiorski, K. (den 19 Maj 2014). Principles and overview of network steganography. *IEEE Communications Magazine Volume: 52*, ss. 225-229.

Mazurczyk, W. (2013). VoIP steganography and its Detection—A survey. *ACM Comput. Surv. 46, 2, Article 20*.

Mazurczyk, W., & Caviglione, L. (2014). Steganography in Modern Smartphones and Mitigation Techniques. *IEEE Communications Surveys & Tutorials (Volume: 17, Issue: 1, Firstquarter 2015)*, 334-357.

Mazurczyk, W., & Caviglione, L. (2015). Information Hiding as a Challenge for Malware Detection. *IEEE Security & Privacy Volume: 13, Issue: 2*, 89-93.

Mazurczyk, W., & Wendzel, S. (December 2017). Information hiding: Challenges for forensic experts. *COMMUNICATIONS OF THE ACM VOL. 61 NO. 1*.

Megías, D. (2020). Data hiding: New opportunities for security and privacy?

Nowakowski, P., Zórawski, P., Cabaj, K., & Mazurczyk, W. (2020). Network covert channels detection using data mining and hierarchical organisation of frequent sets: an initial study. *ARES '20: Proceedings of the 15th International Conference on Availability, Reliability and Security* (ss. 1-10). Virtual Event Ireland: Association for Computing Machinery.

Puchalski, D., Caviglione, L., Kozik, R., Marzecki, A., Krawczyk, S., & Choraś, M. (2020). Stegomalware detection through structural analysis of media files. *ARES '20: Proceedings of the 15th International Conference on Availability, Reliability and Security* (ss. 1-6). Virtual Event Ireland: Association for Computing Machinery.

Rubens, P. (den 29 Augusti 2011). *eSecurity Planet*. Hämtat från Operation Shady RAT Pointing the Way: https://www.esecurityplanet.com/threats/operation-shady-rat-pointing-the-way/

Seo, J. O., Manoharan, S., & Mahanti, A. (2016). A Discussion and Review of Network Steganography. *2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure*

Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech. Auckland, New Zealand: IEEE.

Serrano Pérez, J. D., Rosales, M. S., & Cruz-Cortés, N. (2016). Universal Steganography Detector Based on an Artificial Immune System for JPEG Images. *2016 IEEE Trustcom/BigDataSE/ISPA*. Tianjin, China: IEEE.

Symantec Threat Hunter Team. (den 15 Januari 2021). *Symantec Enterprise Blogs Security*. Hämtat från SolarWinds: Insights into Attacker Command and Control Process: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-sunburst-command-control

Szary, P., Mazurczyk, W., Wendzel, S., & Caviglione, L. (2020). Design and performance evaluation of reversible network covert channels. *ARES '20: Proceedings of the 15th International Conference on Availability, Reliability and Security* (ss. 1-8). Virtual Event Ireland: Association for Computing Machinery.

Templier, M., & Paré, G. (2015). A Framework for Guiding and Evaluating Literature Reviews. *Communications of theAssociation for Information Systems: Vol. 37, Article 6*.

Zielinska, E., Mazurczyk, W., & Szczypiorski, K. (Mars 2014). Trends in Steganography.

Appendix A – Lista med artiklar

Aljamea, M. M., Iliopoulos, C. S., & Samiruzzaman, M. (2016). *Detection Of URL In Image Steganography*. Paper presented at the Proceedings of the International Conference on Internet of things and Cloud Computing.

Brodzki, A. M., & Bieniasz, J. (2019, 18-20 Sept. 2019). *Yet Another Network Steganography Technique Basedon TCP Retransmissions*. Paper presented at the 2019 5th International Conference on Frontiers of Signal Processing (ICFSP).

Bąk, P., Bieniasz, J., Krzemiński, M., & Szczypiorski, K. (2018, 24-27 Sept. 2018). *Application of Perfectly Undetectable Network Steganography Method for Malware Hidden Communication*. Paper presented at the 2018 4th International Conference on Frontiers of Signal Processing (ICFSP).

Cabaj, K., Mazurczyk, W., Nowakowski, P., & Żórawski, P. (2019). *Fine-tuning of Distributed Network Covert Channels Parameters and Their Impact on Undetectability*. Paper presented at the Proceedings of the 14th International Conference on Availability, Reliability and Security.

Carrara, B., & Adams, C. (2016). *A Survey and Taxonomy Aimed at the Detection and Measurement of Covert Channels*. Paper presented at the Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security.

Carrega, A., Caviglione, L., Repetto, M., & Zuppelli, M. (2020, 29 June-3 July 2020). *Programmable Data Gathering for Detecting Stegomalware*. Paper presented at the 2020 6th IEEE Conference on Network Softwarization (NetSoft).

Chauhan, S., Jyotsna, Kumar, J., & Doegar, A. (2017, 9-10 Feb. 2017). *Multiple layer text security using variable block size cryptography and image steganography*. Paper presented at the 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT).

Chourib, M. (2019, 15-19 July 2019). *Detecting Selected Network Covert Channels Using Machine Learning*. Paper presented at the 2019 International Conference on High Performance Computing & Simulation (HPCS).

Francis-Christie, C., & Lo, D. (2016, 10-14 June 2016). *A Combination of Active and Passive Video Steganalysis to Fight Sensitive Data Exfiltration through Online Video*. Paper presented at the 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC).

Geisler, D., Mazurczyk, W., & Keller, J. (2018). *Towards Utilization of Covert Channels as a Green Networking Technique*. Paper presented at the Proceedings of the 13th International Conference on Availability, Reliability and Security.

Goher, S. Z., Javed, B., & Saqib, N. A. (2012, 12-14 Dec. 2012). *Covert channel detection: A survey based analysis*. Paper presented at the High Capacity Optical Networks and Emerging/Enabling Technologies.

Heda, Y., & Shah, R. (2015, 10-11 July 2015). *Covert channel design and detection techniques : a survey*. Paper presented at the 2015 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT).

Jaskolka, J., & Khedri, R. (2011, 4-7 Jan. 2011). *Exploring Covert Channels*. Paper presented at the 2011 44th Hawaii International Conference on System Sciences.

Kaushik, M., Malik, M., & Narwal, B. (2020, 6-8 Nov. 2020). *Developing Malware and Analyzing it Afore & After Steganography with OSINTs*. Paper presented at the 2020 IEEE International Conference for Innovation in Technology (INOCON).

Ker, A. D., Bas, P., Böhme, R., Cogranne, R., Craver, S., Filler, T., et al. (2013). *Moving steganography and steganalysis from the laboratory into the real world*. Paper presented at the Proceedings of the first ACM workshop on Information hiding and multimedia security.

Khader, M., Hadi, A., & Hudaib, A. (2016, 2-4 Aug. 2016). *Covert Communication Using Port Knocking*. Paper presented at the 2016 Cybersecurity and Cyberforensics Conference (CCC).

Kraetzer, C., & Dittmann, J. (2018). *Steganography by synthesis: Can commonplace image manipulations like face morphing create plausible steganographic channels?* Paper presented at the Proceedings of the 13th International Conference on Availability, Reliability and Security.

Kulkarni, Y., & Gorkar, A. (2020, 10-13 Dec. 2020). *Intensive Image Malware Analysis and Least Significant Bit Matching Steganalysis*. Paper presented at the 2020 IEEE International Conference on Big Data (Big Data).

Lehner, F., Mazurczyk, W., Keller, J., & Wendzel, S. (2017, 9-12 Oct. 2017). *Inter-Protocol Steganography for Real-Time Services and Its Detection Using Traffic Coloring Approach*. Paper presented at the 2017 IEEE 42nd Conference on Local Computer Networks (LCN).

Mazurczyk, W. (2013). VoIP steganography and its Detection—A survey. *ACM Comput. Surv., 46*(2), Article 20.

Mazurczyk, W., & Caviglione, L. (2015). Steganography in Modern Smartphones and Mitigation Techniques. *IEEE Communications Surveys & Tutorials, 17*(1), 334-357.

Mazurczyk, W., Wendzel, S., & Cabaj, K. (2018). *Towards Deriving Insights into Data Hiding Methods Using Pattern-based Approach*. Paper presented at the Proceedings of the 13th International Conference on Availability, Reliability and Security.

Megías, D. (2020). *Data hiding: New opportunities for security and privacy?* Paper presented at the Proceedings of the European Interdisciplinary Cybersecurity Conference.

Nowakowski, P., Zórawski, P., Cabaj, K., & Mazurczyk, W. (2020). *Network covert channels detection using data mining and hierarchical organisation of frequent sets: an initial study*. Paper presented at the Proceedings of the 15th International Conference on Availability, Reliability and Security.

Puchalski, D., Caviglione, L., Kozik, R., Marzecki, A., Krawczyk, S., & Choraś, M. (2020). *Stegomalware detection through structural analysis of media files*. Paper presented at the Proceedings of the 15th International Conference on Availability, Reliability and Security.

Pérez, J. D. J. S., Rosales, M. S., & Cruz-Cortés, N. (2016, 23-26 Aug. 2016). *Universal Steganography Detector Based on an Artificial Immune System for JPEG Images*. Paper presented at the 2016 IEEE Trustcom/BigDataSE/ISPA.

Rajba, P., & Mazurczyk, W. (2020). *Exploiting minification for data hiding purposes*. Paper presented at the Proceedings of the 15th International Conference on Availability, Reliability and Security.

Seo, J. O., Manoharan, S., & Mahanti, A. (2016, 8-12 Aug. 2016). *A Discussion and Review of Network Steganography*. Paper presented at the 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech).

Szary, P., Mazurczyk, W., Wendzel, S., & Caviglione, L. (2020). *Design and performance evaluation of reversible network covert channels*. Paper presented at the Proceedings of the 15th International Conference on Availability, Reliability and Security.

Wendzel, S. (2019). *Protocol-independent Detection of "Messaging Ordering" Network Covert Channels*. Paper presented at the Proceedings of the 14th International Conference on Availability, Reliability and Security.

Appendix B – Konceptmatris

Artikel	Identifierat problemområde (Relevans: H (hög) M (medel) L (låg))				
	Exfiltration av data från nätverket	Infiltration av icke önskad data till nätverket	Kommunikations-kanaler för skadlig kod	Svårigheter för tekniskt skydd att upptäcka och förhindra	Försvårat utredande arbete
Aljamea, M. M., Iliopoulos, C. S., & Samiruzzaman, M. (2016)	M	M	L	H	L
Brodzki, A. M., & Bieniasz, J. (2019)			H	M	
Bąk, P., Bieniasz, J., Krzemiński, M., & Szczypiorski, K. (2018)			H	M	L
Cabaj, K., Mazurczyk, W., Nowakowski, P., & Żórawski, P. (2019)	L	L	L	H	L
Carrara, B., & Adams, C. (2016)	M	L	H	H	
Carrega, A., Caviglione, L., Repetto, M., & Zuppelli, M. (2020)	L		M	H	
Chauhan, S., Jyotsna, Kumar, J., & Doegar, A. (2017)				L	
Chourib, M. (2019)	L	L		H	
Francis-Christie, C., & Lo, D.	M			M	

(2016)					
Geisler, D., Mazurczyk, W., & Keller, J. (2018)	L				
Goher, S. Z., Javed, B., & Saqib, N. A. (2012)	L			H	
Heda, Y., & Shah, R. (2015)	L			H	
Jaskolka, J., & Khedri, R. (2011)	L	L		M	
Kaushik, M., Malik, M., & Narwal, B. (2020)	L	L	L	M	
Ker, A. D., Bas, P., Böhme, R., Cogranne, R., Craver, S., Filler, T., et al. (2013)			L	H	M
Khader, M., Hadi, A., & Hudaib, A. (2016)				M	
Kraetzer, C., & Dittmann, J. (2018)	L	L	M	L	
Kulkarni, Y., & Gorkar, A. (2020)	L	L		H	
Lehner, F., Mazurczyk, W., Keller, J., & Wendzel, S. (2017)	L		L	L	
Mazurczyk, W. (2013)	L	L		M	
Mazurczyk, W., & Caviglione, L. (2015)	L	L	L	L	
Mazurczyk, W., Wendzel, S., & Cabaj, K. (2018)				L	

Megías, D. (2020)	L	L			L
Nowakowski, P., Zórawski, P., Cabaj, K., & Mazurczyk, W. (2020)	L	L	L	H	
Puchalski, D., Caviglione, L., Kozik, R., Marzecki, A., Krawczyk, S., & Choraś, M. (2020)	L	M	L	M	
Pérez, J. D. J. S., Rosales, M. S., & Cruz-Cortés, N. (2016)	L			M	
Rajba, P., & Mazurczyk, W. (2020)	L	L	L	M	
Seo, J. O., Manoharan, S., & Mahanti, A. (2016)	L			M	L
Szary, P., Mazurczyk, W., Wendzel, S., & Caviglione, L. (2020)	L		L	L	
Wendzel, S. (2019)	L		L	L	