Skydd av immaterialrätt inom 3D-cad-utveckling med global kollaborering

Patric Gustafsson

Kandidatavhandling

Fakulteten för naturvetenskaper och teknik
Åbo Akademi

2017

Innehåll

Referat

När globala samarbeten görs inom industrier särskilt inom industrier som använder mycket 3D-cad, blir det enkelt problem med immaterialrätt. Företag har hemligheter som de vill skydda men detta kan vara svårt eller nästan omöjligt då man måste ge tillräckligt med information till underleverantörerna så att de kan utföra ett ordentligt jobb. Metoder för att skydda 3D-cad-data och filer där datan finns måste finnas. I denna avhandling behandlas skydd av själva 3D-modellen samt hur de publicerade filerna från 3D-cad-program kan skyddas.

Filstorleken på de publicerad filerna från 3D-cad-verktyg är ofta små och enkla att skicka till utomstående. Att en utomstående, som kan vara t.ex. en konkurrent, får tillgång till de filer kan leda till stora ekonomiska förluster. Företag har därför stort intresse för utvecklingen av nya skydd.

Det unika med fartygsindustrin är att den använder sig av ett stort nätverk av underleverantörer. Dylika problem uppstår inte lika lätt i andra industrier där utvecklingen av hela produkten kan ske på samma plats.

I denna avhandling tas upp olika metoder för att skydda immaterialrätt då globala samarbeten utförs.

KAPITEL 1 Introduktion

Globala samarbeten inom fartygsindustrin växer hela tiden. Inom denna industri har det blivit mycket vanligt att man använder sig av underleverantörer för att designa och utveckla fartygets delar. Här uppstår ett problem då skeppsvarven inte vill dela med sig av hela sin design till sina underleverantörer, detta för att kunna skydda sin immaterialrätt. För att undkomma stöld vill företag kunna skydda sina 3D-cad (Computer Aided Design) modeller då de skickas till deras underleverantörer. Detta kan göras manuellt men i bästa fall borde programvaran ha möjlighet efter minimala instruktioner kunna göra detta själv.

Problemet att skydda immaterialrätt för 3D-cad-filer är tvådelat: Första delen av problemet är att när filen öppnas i något program som visar den måste de detaljer som är hemliga på något sätt filtreras bort. Andra delen av problemet består av att skydda själva filen som öppnas. Om denna kopieras och skickas utanför företaget kan obehöriga få all designinformation som de behöver för att kunna stjäla någon viktig detalj från designen. Den första delen av problemet behandlas i Kapitel 2, medan den andra delen behandlas i Kapitel 4.

I avhandlingen behandlas Cadmatic som fallstudie. Cadmatic är en av de största utvecklarna av 3D-cad-programvara för fartygsindustrin. Inom kundkretsen ingår bl.a. Meyer Turku Oy och Drydocks World Dubai. Skeppsvarv har mycket immaterialrätt som de vill undanhålla från konkurrenter och eventuella illvilliga underleverantörer. Enligt skeppsvarven är följande en del av det som de vill kunna skydda: skeppets skrov, propellrarnas design, bränslesystem, trappuppgångar och andra detaljer. Metoder för att skydda skeppets skrov har det inte forskats mycket om, men däremot finns det forskning för om hur mindre detaljer ska skyddas.

I denna kandidatavhandling tar jag endast upp de tekniska lösningarna på dessa problem. När man behandlar immaterialrätt på ett mera allmänt plan måste man även tänka på de lagliga åtgärder man kan ta till för att skydda immateriella rättigheter, men detta är utanför den här avhandlingens område.

1.1 Avhandlingens syfte

Avhandlingens syfte är att ta reda på vilka olika tekniker det finns för att skydda immaterialrätt inom 3D-cad-utveckling och speciellt då utvecklingen sker med hjälp utav globala samarbeten mellan företag.

1.2 Allmänt om immaterialrätt

I detta stycke beskrivs kort vad immaterialrätt är och vilka olika delar som i allmänhet ingår i skydd av immaterialrätt.

1.2.1 Vad är immaterialrätt?

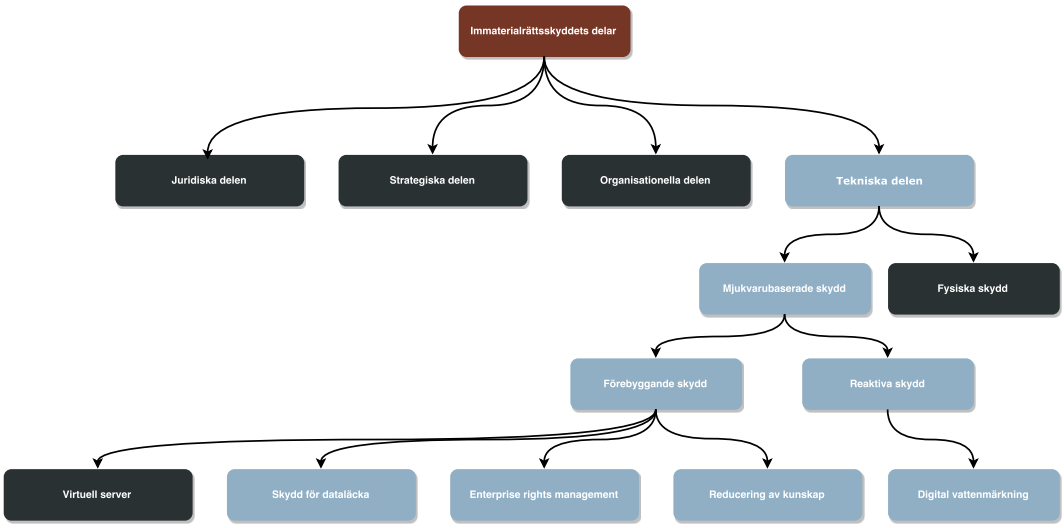
Enligt EU [1] består immaterialrätt av två delar: den ena delen är den industriella delen, d.v.s., uppfinningar (patenter), varumärken och industriell formgivning. Den andra delen är den icke-industriella delen. I denna ingår den konstnärliga och litterära äganderätten. EU definierar ännu [1] konceptet för "företagshemligheter", dessa är inte direkt skyddade under EU:s lagstiftning utan lagarna skiljer sig från land till land.

När jag i denna avhandling behandlar skydd av immaterialrätt så är det den industriella delen samt företagshemligheterna som avses. Inom fartygsindustrin kan många detaljer ses som företagshemligheter då de inte är patenterade.

1.2.2 Immaterialsrättsskyddets olika delar

I detta stycke ges en överblick i vad som ingår i immaterialrätt och vilka saker som tas i denna avhandling. I Figur 1.1, som är tagen från Paredis et al. [2], syns vilka olika delar som allmänt ingår i immaterialrätt. De delar som har ljusare färg är de delar som tas upp i denna avhandling.

Figuren visar att de skydd som jag behandlar i avhandlingen är de mjukvarubaserade skydden. Ett viktigt mjukvarubaserat skydd inom 3D-cad-utveckling är att reducera hur mycket data som en viss person har åtkomst till. Då kan man vara säker på att konfidentiella data inte visas för dem som inte har tillgång till dem. I Kapitel 2 behandlar jag skydd av själva 3D-modellen. Sedan i Kapitel 3 behandlar jag Cadmatics egen implementation av det som jag beskriver i Kapitel 2. Eftersom



Figur 1.1: Översikt av immaterialrättsskyddets olika delar

Cadmatic redan har implementerat en del av de metoderna så behandlar jag det ganska kortfattigt. Även vattenmärkning behandlas kort vilket hör till kategorin att reaktivt skydda data.

Skydd av dataläckor samt ERM-system behandlar jag i Kapitel 4. Detta kapitel är mera ingående eftersom företag inom fartygsindustrin ofta använder sig utav 3D-cad-filer som skickas till underleverantörer och då är risken för att en dataläcka sker stor. I slutet av kapitlet finns en sammanfattning av alla teknikerna för att skydda 3D-cad-filer samt deras för- och nackdelar.

KAPITEL 2 Metoder för att skydda 3D-cad-data

Inom 3D-cad utveckling finns ofta i modellerna företagshemligheter och detaljer som är skyddade av immaterialrätt.De metoder som jag har valt att ta upp i detta stycke är baserade på de som Stjepandic et al. [3] tog upp i deras undersökning om vilka olika metoder som existerar för att skydda immaterialrätt inom 3D-cad-data. I huvudsak finns tre olika metoder för att skydda 3D-cad-data; att ta bort 3D-cad-data, att förenkla 3D-cad-data och att vattenmärka 3D-cad-data. För att relatera dessa metoder tillbaka till den allmänna delen av immaterialrättsskydd, vilken jag beskrev i stycke 1.2.2, så kan borttagning och förenkling av data ses som reducering av kunskap medan vattenmärkning förstås är relaterat till vattenmärkningen i den allmänna delen.

2.1 Borttagning av 3D-cad-data

2.1.1 Manuellt

Manuell borttagning av data har visats av b.la. Paredis et al. [2] att vara det bästa sättet att skydda 3D-cad-data. Orsaken är den att då kan man vara säker på att exakt det som man inte vill visa till andra är borttaget. En stor nackdel är att det är väldigt tidskrävande att göra detta manuellt. Alla 3D-cad-system erbjuder denna möjlighet eftersom att lägga till och ta bort saker är en av grundfunktionerna som de programmen erbjuder.

2.1.2 Automatiskt

Med automatiskt borttagning menas inte att det borttagningen ska ske helt på automatik, utan det som menas är att den som använder programmet inte själv ska behöva ta bort detaljerna utan ska kunna ge instruktioner till programmet vilken data som ska tas bort och sedan ska programmet ta bort data själv. Cadmatics COS-server som är ett system för att distribuera ut 3D-cad-modeller mellan olika

företag och företagens underleverantörer, har en funktion för att ta bort data automatiskt efter att man i COS-server har definierat vad som ska tas bort. Jag beskriver COS-server djupare i stycke3.1.1.

2.2 Förenkling av 3D-cad-data

Att förenkla data kan precis som med borttagning av data göras på två olika sätt. Antingen manuellt eller automatiskt. Att förenkla data är inte samma sak som att ta bort den. Med förenkling så finns data ännu kvar men i en simplare form från vilken det oftast är svårare att utläsa detaljer och genom detta skydda immaterialrätt. I Cadmatics fall använder de sig av förenkling men avsikten där är inte att skydda immaterialrätt utan att spara på resurser eftersom att rendera hela 3D-modellen med fulla detaljer är resurskrävande.

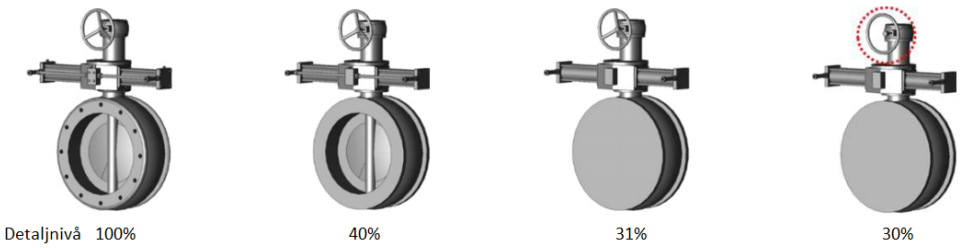
2.2.1 Manuellt

Manuell förenkling av data erbjuder t.ex. programmet Solidworks från Dassault Systems [4]. Programmet kan fylla i tomma ytor och lägga till objekt som täcker över det som man vill hålla hemligt. Om man har en liten modell så är detta ganska enkelt, men om man jobbar med större modeller, så blir detta jobb igen väldigt mödosamt att göra manuellt.

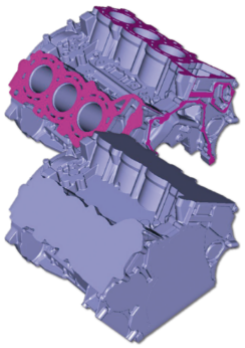
2.2.2 Automatiskt

Automatisk förenkling av data med avsikten att skydda immaterialrätt har utvecklats av b.la. Sonjoo et al. [5] samt Lee och Lee [6]. Förenklingen fungerar genom att den rangordnrar vilka objekt som är viktiga och tar sedan bort objekten i tur och ordning enligt vissa regler. I 2.1 visas hur förenkling av ett munstycke skulle kunna se ut.

Att skydda immaterialrätt med endast förenkling är oftast endast möjligt då man jobbar med enskilda modeller av något slag. Ett helt fartyg är inte möjligt att förenkla så lång att några hemliga detaljer skulle kunna gömmas. I Figur 2.2.2 visas hur programmet 3D-Evolution från Coretechnologie, vilket nämndes tidigare i detta stycke, använder sig av förenkling för att gömma detaljer i ett motorblock. Programmet åstadkommer detta genom att söka upp tomma hål och fylla i dem.



Figur 2.1: Olika förenklingsnivåer på ett munstycke



Figur 2.2: Förenkling av ett motorblock

2.3 Vattenmärkning av 3D-cad-data

Att vattenmärka saker är inget nytt. Foton och dokument har länge haft möjligheten att vattenmärkas. För en djupare genomgång av vattenmärkning för andra saker än 3D-cad-data se t.ex. Hartung och Kutter [7] som 1999 tog upp vattenmärkning av olika digitala media. Att vattenmärka någonting innebär att allmänt att sätta till någon liten detalj så att en sak, t.e.x ett dokument, kan sammankopplas med ett visst företag eller person.

Metoder för att vattenmärka 3D-cad-data har utvecklats, t.ex. utav Wu et al. [8]. Idén med vattenmärkning för 3D-cad är likadan som för vanlig vattenmärkning, t.ex. med dokument. Det som sker är att någon detalj i 3D-objektet modifieras på ett sådant sätt att vattenmärkningen kan vid ett senare tillfälle fås ut från modellen. Själva modellen ändras inte märkbart, detta så de arbete som designers eller ingenjörer utför på modellen inte ska påverkas.

En stor nackdel med vattenmärkning enligt Cat et al. [9] är att vattenmärkning kan inte användas för att skydda immaterialrätt på något sätt utan kan endast användas för att påvisa att immaterialrättsstöld har begåtts.

Enligt Stjepandic et al. [3] finns det i nuläget inte några kommersiella system som har implementerat vattenmärkning för 3D-cad-data utan det är endast i teorin som det har gjorts forskning.

KAPITEL 3 Immaterialrättsskydd vid Cadmatic

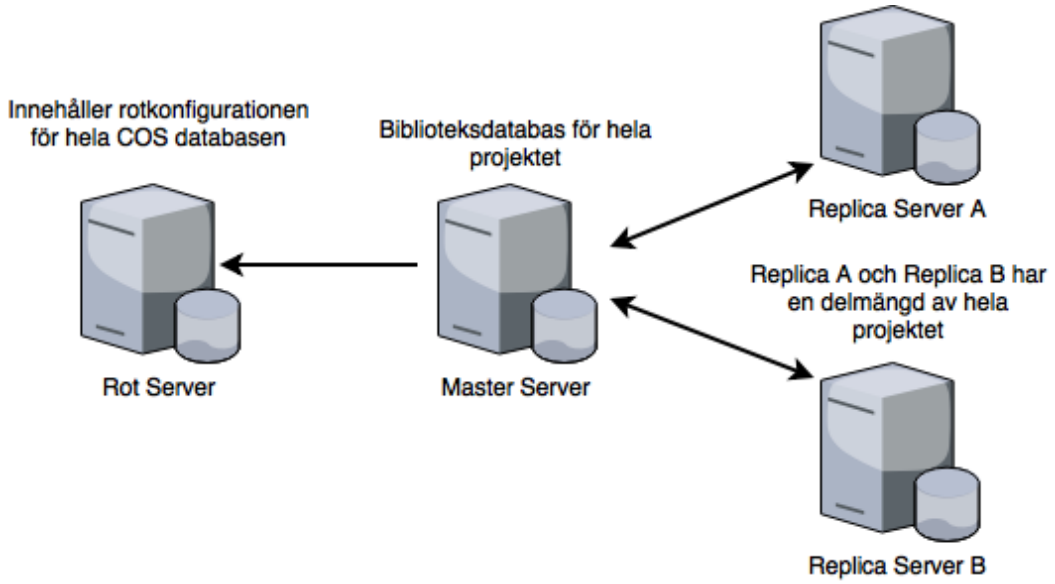
I detta stycke beskriver jag hur de tekniker som jag beskrev i Kapitel 2 tillämpas hos Cadmatic. Först beskriver jag COS-server som har en funktion för att automatiskt ta bort 3d-cad-data vilket gör det möjligt för företag att skydda sin immaterialrätt. Att ta bort 3D-cad-data beskrev jag i Kapitel 2 som en av de metoder som finns för att skydda immaterialrätt inom 3D-cad-utveckling. Förenkling av 3d-cad-data sker i alla av Cadmatics 3d-cad-program och den sker automatiskt. Till slut tar jag upp eBrowser vilket är ett program som används för att visa exporterade modeller (3D och 2D) från något av Cadmatics design-program, exempelvis Cadmatic 3D Outfitting design [10]. Jag behandlar eBrowser eftersom den framhäver den andra delen av det problem som jag beskrev i Kapitel 1.

3.1 COS Server

COS (Cadmatic Object Storage) är en databasserver som används för att distribuera 3D-modeller mellan olika företag som samarbetar med samma modell. Strukturen är hierarkisk vilket innebär att om en modell uppdateras eller ändras på en server längre ner i hierarkin så kommer dessa uppdateringar att röra sig uppåt i strukturen. På detta sätt hålls alla modeller uppdaterade. Ett exempel på hur en simpelt COS nätverk kan se ut finns i Figur 3.1.

3.1.1 Filtrerad kopiering

I många fall vill företag inte att underleverantörer ska ha tillgång till hela 3D-cad-designen. COS-server erbjuder då en funktion som kallas för filtrerad kopiering. Med denna funktion kan användare välja hur stor del av modellen som underleverantörer ska få tillgång till. Det är möjligt att ge tillgång till endast en delmängd av det data som finns på den originella servern. Utöver detta kan den som delar ut modellen definiera ett skyddat område som inte skall visas för någon underleverantör. Båda dessa koncept illustreras i Figur 3.2. I figuren visas överst en sidobild



Figur 3.1: Struktur för ett simpelt COS nätverk

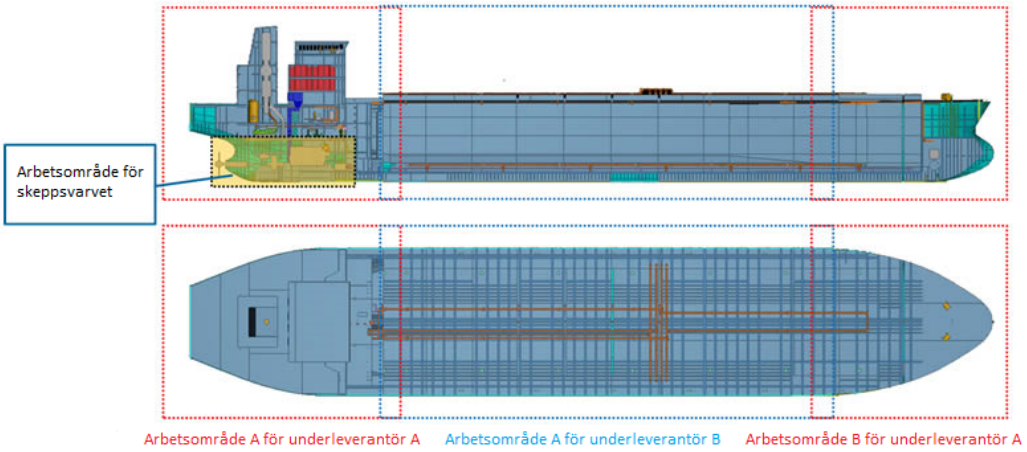
som beskriver hur indelningen av ett fartyg är gjort mellan tre olika aktörer: *A*, *B* samt ett skeppsvarv. Ur bilden kan man se att *A* endast har tillgång till aktern och fören, medan *B* har tillgång till den mellersta delen av fartyget. Det utmärka området för skeppsvarvet är det så kallade hemliga området, vilket i detta fall är motorrummet. Varken *A* eller *B* kommer att ha tillgång till det. Märkt att tillgång till ett område ges endast till båda underleverantörerna då en överlappning finns i det området.

Från det område som är definierat som hemligt kommer ingenting att kopieras till någondera av underleverantörerna. De kommer inte heller att kunna komma åt någon annan del av fartygs-modellen än den som de har fått replikerad till sig. Det hemliga området kommer att visas som en svart låda runt den region som är hemlig.

3.2 eBrowser

Från Cadmatics program kan man enkelt exportera ut en förenklad modell som man kan öppna med programmet eBrowser. Programmet (eBrowser) är till för att ge ingenjörer och designers enkel tillgång till 3D-modellen utan att behöva öppna ett av de tyngre programmen. Programmet har således inte funktioner för att utveckla nya modeller utan kan endast vissa modellerna. Det är möjligt att i programmet bl.a. mäta avstånd mellan objekt.

Filerna som exporteras ut från Cadmatics program och som sedan eBrowser an-



Figur 3.2: Filtrerad kopiering ger tillgång till endast en del av modellen

vänder sig av är i de flesta fall väldigt små vilket gör det mycket lätt för någon att skicka filerna till utomstående som inte skall ha tillgång till dem. För tillfället har Cadmatic inget skydd för dessa filer och de går enkelt att öppna även med gratisversionen av eBrowser som man kan ladda ned från Cadmatics hemsida.

Ett vanligt användningsområde för eBrowser filer är att filerna skickas till diverse underleverantörer som sedan gör något vidare jobb med filerna. Här uppstår den andra delen av det problem som jag beskrev tidigare i Kapitel 1. I nästa kapitel behandlar jag några lösningar till det problemet.

KAPITEL 4 Skydd av eBrowser filer

För att ha ett ordentligt skydd av immaterialrätt räcket det inte med att endast skydda själva 3D-modellen. Det kan t.ex. finnas fall då någon glömmer att aktivera en region som hemlig fast den skulle vara det och då kan denna fil skickas till utomstående som sedan kan se den hemliga regionen. Därför behövs det även skydd för själva filen. Detta stycke behandlar andra delen av problemet som jag beskrev i stycke 1. En kort översikt samt motivering av vilka tekniker som tas upp i detta kapitel finns i stycke 4.1. För att igen relatera detta tillbaka till den allmänna modellen för att skydda immaterialrätt så behandlar jag i detta stycke delarna ERM-system och skydd av dataläckor.

4.1 Tekniker samt motivering

I detta stycke tar jag upp vilka tekniker som jag har undersökt samt motiverar varför jag har valt just dessa tekniker och inte någon annan teknik.

- ERM (Enterprise Rights Management). Enligt Stjepandic et al. [3] anses ett fullständigt ERM system vara det bästa sättet att skydda filer och dokument inom företag, just av denna anledning valde jag att ta med ERM. Jag behandlar ERM-system i stycke 4.2.f
- Lösenordsskydd. Detta finns implementerat i många system och är väldigt vanligt, se b.la. Navisworks och Microsofts skydd för Office-filer. [11], [12]. Lösenordsskydd behandlar jag i stycke 4.3.
- Utgångsdatum. Detta har varit efterfrågat av Cadmatics kunder. Det finns även implementerad i både Navisworks och i Microsoft skydd för office-filer, så det finns ett klart behov för utgångsdatum. Detta behandlar jag djupare i stycke 4.4.

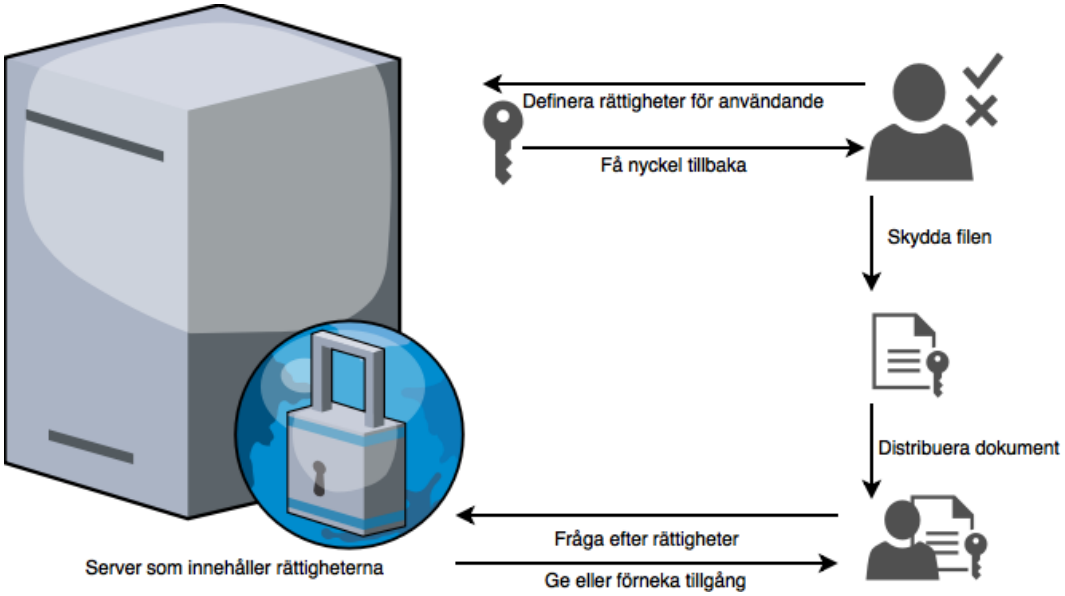
Att kryptera filerna är förstås ett viktigt moment för att ge bättre säkerhet åt filerna. Genom hela kapitlet antar jag att det finns något sätt som filerna krypteras

på färdigt och jag går därför inte djupare in på hur krypteringen skulle implementeras.

4.2 Enterprise Rights Management

Enterprise Rights Management (ERM) definieras enligt Stjepandic et al.[3] som de tekniker som ingår för att skydda immaterialrätt inom företag. Kommersiella ERM system är b.la. Adobe LifeCycle Manager [13] samt Microsoft Azure Rights Management [14]. Beskrivningen som följer är baserat på det som skrevs av Stjepandic et al.[3].

Ett ERM-system fungerar genom att det finns en server där alla användare samt vilka filer de har rättigheter till finns sparade. När en fil ska distribueras väljer den som distribuerar filen först vilka som ska ha rättighet att komma åt filen och sedan kan filen distribueras. När någon sedan vill öppna filen kontaktas servern för att verifiera om användaren som tar kontakt har rättigheter till filen. Se figur 4.1 för en grafisk beskrivning av detta. Rättigheterna kan kontrolleras på flera olika sätt, t.ex. genom vanligt användarnamn och lösenord.



Figur 4.1: Principen för en ERM baserad lösning

Att ta denna lösning i bruk skulle kräva störst förändringar av alla de metoder som föreslås här. Däremot ger den bra säkerhet eftersom en användare måste autentisera sig innan den använder sig utav filen. Eftersom den person som distribuerar filen kan välja vilka som får tillgång till filen är risken liten att någon som man inte litar på skulle få tillgång till den.

Nackdelar med ERM-system är att programmet måste ta kontakt med servern vid varje uppstart. Om ännu en server används som endast kan nås inifrån ett företagsnätverk så kan detta skapa problem om användare vill jobba t.ex. hemifrån eller på platser där det saknas kontakt med nätet. En lösning till det första problemet är att dela ut så kallade tidsbiljetter till användare. Dessa skulle ge tillgång till programvaran under en viss tidsperiod, t.ex. i Adobes Lifecycle [13] gjordes detta genom att ge användare en fyra-timmars period under vilken de kunde jobba utan nätkontakt. När den perioden sedan tog slut kontaktades servern på nytt för att verifiera rättigheterna. Den andra delen av problemet, att inte kunna jobba utifrån företagsnätverket, kan lösas genom att använda en VPN-anslutning till företaget. Att använda en säker anslutning och att kunna verifiera att den server man kopplar upp till faktiskt är den rätta är viktigt. Detta diskuteras i stycke 4.2.1.

4.2.1 Kryptering av anslutning och certifikat

Om servern använder sig av okrypterad anslutning finns det möjlighet att en användare kan förfalska anslutningen (även kallat "spoofing", se IDG:s IT-ordbok [15]), och på detta sätt kringgå utgångsdatumet. För att kunna skydda anslutningen måste den alltså vara krypterad. Det finns olika krypteringsmetoder beroende på vilket protokoll som används mellan klienten och servern. Enligt Pandya et al. [16] är SSL (Secure-Socket-Layer) en vanlig krypteringsstandard som används för att göra kommunikation mellan en server och en klient säker.

Vid användning av SSL används även någonting som kallas för **certifikat**. Dessa används för att verifiera att anslutningen som används är den rätta. Om inte rätt certifikat hittas så godtas inte anslutningen även om den skulle vara krypterad. Certifikat är ett sätt att motarbeta att någon skulle förfalska anslutningen.

Förfalskade certifikat är ett problem som förekommer, detta har b.la. gjorts studier av Levillain et al. [17] som kom fram till att ungefär 5 procent av alla certifikat som används av webbsidor är förfalskade. Georgiev et al. [18] visade de att inte bara förfalskade certifikat är ett problem utan även felaktig implementering av SSL kan förekomma. För att undvika båda dessa problem är det rekommenderat att man endast använder sig utav standard SSL-bibliotek som finns tillgängliga och inte utvecklar egna lösningar.

Inte ens med färdiga bibliotek kan man vara 100-procent säker på att det inte finns fel i implementationen. Ett exempel på detta är i fallet med OpenSSL, som är ett öppen-källkodsprogram som implementerar SSL. Programmet innehöll ett

fel som möjliggjorde för vem som helst att förfalska anslutningen och på så viss komma åt användares data som de inte skulle ha tillgång till. Felet är idag rättat och OpenSSL borde vara säkert att använda. Men fallet visar att man inte ens kan fullt lita på offentliga implementationer fast de har kollats av flera hundra olika utvecklare över en lång tid.

4.3 Lösenordsskydd för eBrowser filer

Att använda lösenord för att skydda filer är kanske det vanligaste sättet. Det finns många olika sätt att implementera lösenord. Nedan finns en uppräkning av olika metoder som anses vara relativt vanliga sätt att implementera lösenord på. Utav dessa har jag valt ut några metoder att beskriva närmare. Urvalet baserar sig på hur bra en viss metod passar in för filer som ska användas med många underleverantörer, vilket eBrowser filer ofta användas för. De fyra olika lösenordsskydd som jag tar upp här baseras på en del av de metoder som Pandya et al. [16] beskriver.

- Vanligt lösenord. Fungerar genom att den som distribuerar ut filen väljer ett lösenord för att skydda filen. Detta är enkelt att implementera och lätt för användare att förstå.
- Engångslösenord. En lista med lösenord skapas där varje lösenord kan användas endast en gång. Detta gör det svårt att gissa lösenordet och om ett lösenord råkar komma ut så kan det ändå bara användas en gång. Detta skulle kunna ske genom att lösenordet distribueras via t.ex. SMS.
- Grafiskt lösenord. Ett grafiskt lösenord fungerar genom att användaren skulle rita en bild och denna skulle användas som lösenord. För att låsa upp filen skulle bilen ritas på nytt.
- Biometriskt lösenord. Upplåsning av filen skulle fungera genom ögonskanning eller fingeravtryck. Om man på förhand vet vilka som ska ha tillgång till filen kan detta kombineras med ERM-systemet för att verifiera t.ex. fingeravtryck på basen av användare.

Fördelarna med lösenord är att de är enkla att implementera och teoretiskt kan man göra krypteringen för den fil man vill skydda så stark som möjligt. Nackdelarna med lösenord har studerats av b.la. Florencio et al. [19] som kom fram till att de största nackdelarna som lösenord allmänt har är inte tekniska utan beror mera på hur lösenorden används. Problem som nämns är b.la. att användare enkelt glömmer

lösenord samt att de är enkla att dela ut till andra människor. Florencio et al. [19] visade ännu att många användare har en tendens att återanvända lösenord på många ställen vilket är ännu en säkerhetsrisk.

Ett helt vanligt lösenord har alltså många nackdelar. Fördelen är att lösenord är enkelt att implementera och det behövs ingen extra hårdvara för att ta i bruk vanliga lösenord.

Engångslösenord ger bättre säkerhet eftersom ett lösenord endast går att använda en gång. Dessutom behöver användare inte komma ihåg några lösenord då ett nytt skapas varje gång. Nackdelen är att det krävs extra hårdvara för att sätta igång ett helt sådant här system. Detta system fungerar även bara då det på förhand är känt vem som ska ha tillgång till filen, eftersom lösenordet måste skickas till just en av de personerna som ska ha tillgång till filen.

Grafiska lösenord har samma nackdelar som med vanliga lösenord. Att använda ett grafiskt lösenord är inte realistiskt då filen som ska skyddas med lösenordet ska kunna delas ut åt andra. Det är också enkelt att dela ut detta lösenord till obehöriga eftersom det endast är en bild.

Biometriska lösenord har den fördelen att de är unika till varje person samt att de är svåra att skicka till obehöriga. I dagsläget är det fingerskanning som har fått mest spridning men i framtiden kan tänkas att även ögonskanning skulle kunna användas. Även med biometriska lösenord (som med grafiska eller engångslösenord) måste det på förhand vara känt vem som ska ha tillgång till filen eftersom systemet måste kunna verifiera att den personen har tillgång till filen. Även extra hårdvara måste införskaffas för att kunna använda biometriska lösenord, exempelvis hårdvara för att utföra fingerskanning.

4.4 Utgångsdatum för eBrowser filer

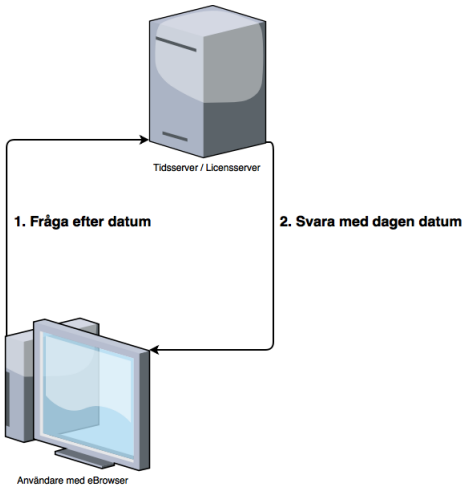
För att implementera utgångsdatum måste en datumkoll ske på något sätt. I huvudsak finns det två metoder för att göra detta. Den ena metoden är att kontrollera datumet med datorns inbyggda hårdvaruklocka och på det viset få en lösning som fungerar helt utan nätkontakt. Denna lösning tar jag upp i stycke 4.4.2.

En annan metod är att använda en server som programmet kopplar upp till för att göra tidskollen, denna metod tar jag upp i stycke 4.4.1.

4.4.1 Server för verifiering av utgångsdatum

Att använda en server dit användare kopplar upp sig varje gång innan de använder sig av programvaran kan vara en möjlighet. Detta har implementerats i de ovan nämnda systemen från både Adobe och Microsoft. Detta kan kombineras med ERM-systemet som jag beskrev tidigare i stycke 4.2 eller så kan en fristående server användas. Skillnaden blir att om ERM-systemet inte används så kan vem som helst öppna filen så länge som utgångsdatumet inte har passerats.

För att kunna veta om utgångsdatumet har passerat skulle användarna varje gång innan de använder sig av programvaran koppla upp sig till en server som skulle bekräfta om utgångsdatumet har passerat eller inte. Om datumet har passerats skulle användarna inte längre ha möjlighet att öppna filen. I Figur 4.2 beskrivs hur serverstrukturen skulle se ut.



Figur 4.2: Hur förfrågan efter datum skulle ske i praktiken

Om detta används i kombination med ERM-systemet så är säkerheten lika bra som om man använder ERM-systemet ensamt. Ifall en fristående server används som inte använder sig utav rättigheter blir säkerheten lite sämre, eftersom vem som helst kan öppna filen så länge som utgångsdatumet inte har passerats.

Nackdelar med att använda en server är i princip de samma som med ERM-systemet så de tas inte upp här igen, nackdelarna med ERM-system beskrev jag i stycke 4.2.

4.4.2 Offline lösning för utgångsdatum

I många sammanhang har man inte tillgång till nätet då man vill jobba med något. Då måste möjligheten ges att även då kunna öppna modellen i eBrowser. Ett program som innehåller denna funktionalitet är det tidigare nämnda NavisWorks, mera information om hur utgångsdatum har implementerats där finns inte tillgängligt. NavisWorks lösning gick även enkelt att kringgå genom att jag flyttade klockan i operativsystemet bakåt. I en offline lösning måste ändå datumkollen ske med hjälp utav hårdvaruklockan, så redan här finns en märkbar säkerhetsrisk.

Datumet måste alltså sparas offline på något sätt. För att göra det svårare att komma åt datumet måste det sparas i ett krypterat format. Det är ändå möjligt att komma åt datumet eftersom dekrypterings-nyckeln måste sparas någonstans i filen, men att komma åt nyckeln är inte någon enkel process om den som letar efter nyckeln inte vet var den finns sparad. Säkerheten blir alltså inte den bästa eftersom det nu teoretiskt är möjligt att komma åt datumet och ändra det. Däremot ur en användares synvinkel är denna metod ganska bra då den tillåter att hen jobbar utan nätkontakt.

Det finns ingen generell metod för var eller hur datumet ska sparas. En idé är att använda samma metod som programvara som använder sig utav en försökstid gör, t.ex. Photoshop [20], som har en försökstid på 30-dagar. Photoshop har ingen dokumentation över hur de implementerar försökstiden men enligt Khanse [21] används ofta gömda filer eller registernycklar i praktiken för att spara utgångsdatumet.

Säkerheten för detta system är inte särskilt bra eftersom det finns många guider och artiklar på nätet för hur man ska komma runt dessa åtgärder. Fördelen är att det är relativt enkelt att implementera dessa metoder och ingen ny hårdvara behöver anskaffas, att programmet nu även går att använda offline ses som en fördel. Ett problem som uppstår är att en skicklig användare kan injektera programkod i filbinären och på så sätt komma förbi datum- eller licenskollen. Detta har gjort av b.la. Tevfik et al. [22]. För att skydda program mot detta har t.ex. Stanley et al.[23] utvecklat metoder för att göra koden mera svårförstådd, så att injiceringen av kod inte ska vara lika lätt.

4.5 Implementationsmöjligheter vid Cadmatic

I princip är varje av de tekniker som jag har tagit upp i detta kapitel möjlig för Cadmatic att implementera. Vilken av teknikerna som i slutändan väljs för implementering beror främst på vilka säkerhetskrav kunder ställer fram. Nedan är en kort genomgång av vad som skulle krävas för att Cadmatic skulle kunna implementera en viss teknik.

ERM, För att ta i bruk ERM skulle en rättighetsserver behövas, vilket beskrevs i stycke 4.2. I nuläget har Cadmatic inget som liknar en rättighetsserver så detta skulle behövas anskaffas. I verkligheten skulle antagligen varje kund ha en egen rättighetsserver som eBrowser skulle koppla upp till för att kolla rättigheterna. I stycke 4.2 beskrev jag för och nackdelarna med ERM-system.

Lösenord. Tidigare i detta kapitel beskrev jag fem olika sorters lösenord, se stycke 4.3. Att ta i bruk någon av de lösenordslösningar som inte kräver någon extra hårdvara skulle vara ganska enkelt för Cadmatic. Att ta i bruk biometriskt- eller engångslösenord skulle kräva hårdvaruanskaffningar. Båda dessa lösenordsskydd beskrev jag i stycke 4.3.

Utgångsdatum. Detta är något som är efterfrågat av Cadmatics kunder så detta skulle ha prioritet för implementering. En offline lösning skulle antagligen tas först i bruk och sedan om större säkerhetskrav ställs på lösningen så kan den server-baserade lösningen implementeras, se stycke 4.4 för en beskrivning av offline lösningen och stycke 4.4.1 för beskrivningen av den server baserade lösningen. I Cadmatics fall så har de redan funktionalitet i eBrowser att koppla upp till en licensserver så samma funktionalitet skulle kunna användas för att kolla utgångsdatumet. Utgångsdatum beskrev jag i stycke 4.4.

Det år även möjligt att använda en kombination av dessa tekniker. En kombination skulle vara att som autentiseringsmetod för ERM använda biometriskt-lösenord. Genom att kombinera teknikerna på detta sätt går det att få ut de bra egenskaperna från båda metoderna och på samma gång undkomma en del av nackdelarna.

KAPITEL 5 Olösta problem i immaterialrättsskydd

Fartygsindustrin är speciell i det avseende att de cad-modeller som företag vill skydda är ofta väldigt stora, d.v.s modellen inkluderar många olika objekt, i vissa fall ett helt fartyg. I detta stycke tar jag upp två olösta problem gällande immaterialrätt upp. Det första, att skydda skeppets skrov, är unikt till fartygsindustrin. Det andra, analoga hålet, är en princip som dyker upp i de flesta fall då man försöker skydda digitala medier.

5.1 Skydd av skeppets skrov

Inom 3D-cad för fartyg uttrycks skeppets skrov oftast med hjälp av en så kallad NURBS (Non-Uniform Rational B-Spline) yta. Detta finns beskrivet av b.la. Swee et al. [24]. Hittills har det inte forskat mycket i hur man skall göra för att skydda skrovet på ett sådant sätt så att den inte går att stjäla eller kopiera om någon skulle få tag på en modell som innehåller skrovet. Problemet är att ytan inte på något enkelt sätt går att förenkla eller tas bort, vilket är möjligt med mindre detaljer, t.ex. med de metoder som jag beskrev i Kapitel 2. Även om man skulle lyckas med att på något sätt förenkla skrovet eller ta bort det från modellen så är det ändå möjligt att med hjälp utav själva metallstrukturen för skrovet återskapa skrovet genom att använda laserskanning.

5.2 Analoga hålet

Analoga hålet [25] beskrivs av Electronic Frontier Foundation (EFF) som det hål som uppstår då t.ex. musik eller bilder måste gå genom något analogt medium för att kunna visas åt en människa. I det tillfället kan människan helt enkelt spela in ljudet eller fotografera bilden utan det finns något som varken hårdvara eller mjukvara kan göra åt saken. Detta problem finns även vid utveckling av 3d-cad-modeller. Modellerna måste även visas på skärmen och då finns det inget som kan stoppa en hängiven tjuv för att ta en bild eller kopiera exportera modellen

från programmet. Kvaliteten blir förstås lidande om tjuven använder sig utav en kamera eller liknande för att kopiera modellen men om modellen exporteras ut från programmet så finns i princip allt material som behövs för att stjäla modellen eller någon detalj från den. Analoga hålet kan delvis stoppas genom att använda en eller flera av de metoder som jag beskrev i Kapitel 4. Ingen av metoderna stoppar ändå en anställd som redan har rättighet till modellen från att kopiera eller exportera den vidare.

KAPITEL 6 Diskussion och sammanfattning

Att skydda 3D-cad-data samt de filer som den data befinner sig i är ingen lätt utmatning. Detta försvåras ännu genom att globala nätverk av underleverantörer används vid utveckling av fartyg. I denna avhandling har jag tagit upp vilka olika metoder det finns just nu för att skydda 3D-cad-data samt hur de filer där den data finns kan skyddas. Ingen av de alternativa metoderna jag tog upp för 3D-cad-data är speciellt lämpad för fartygsutveckling och inga metoder verkar i nuläget existera heller, här krävs alltså mera forskning för att utveckla bättre metoder för att skydda immaterialrätt inom fartygsutveckling.

För att skydda filerna undersökte jag flera olika tekniker som alla kan tillämpas hos Cadmatic, även om vissa metoder, t.ex. biometriska-lösenord eller ERM-system ger objektivt bättre skydd. Inom detta område skulle mera forskning kunna göras som skulle ta reda på flera alternativa metoder för att skydda filer inom företag.

Litteraturförteckning

[1] *IMMATERIELLA, INDUSTRIELLA OCH KOMERSIELLA RÄTTIGHETER*, Europeiska Uniionen, 2017.

[2] C. J. J. Paredis, C. Bishop, and D. Bodner, "Intellectual property protection and secure knowledge management in collaborative systems engineering," *Procedia Computer Science*, vol. 16, p. 572, 2013.

[3] M. Grau, H. Liese, and J. Stjepandic, "Intellectual property protection in the maritime industry - state-of-the-art review and solution approaches," *International Conference on Computer Applications in Shipbuilding*, vol. 3, pp. 181–197, Sep 2013.

[4] Solidworks defeature. Dassault Systems. (Hämtad: 6.3.2017). [Online]. Available: "http://help.solidworks.com/2016/English/SolidWorks/sldworks/c_Defeature_Tool.htm"

[5] K. Sonjoo, K. B. Chul, H. Hojing, M. Duhwan, and H. Soonhung, "Enhanchement of equipment information sharing using three-dimensional computer-aided design simplification and digital catalog techniques in the plant industry," *Concurrent Engineering: Research and Applications*, vol. 24, pp. 275–289, 2016.

[6] L. S. Hun and L. Kunwoo, "Simultaneous and incremental feature-based multiresolution modeling with feature operations in part design," *Computer Aided Design*, vol. 44, pp. 457–483, 2012.

[7] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1079–1107, Jul 1999.

[8] H.-T. Wu and Y.-M. Cheung, "A fragile watermarking scheme for 3d meshes," in *Proceedings of the 7th Workshop on Multimedia and Security*, ser. MM&Sec '05. New York, NY, USA: ACM, 2005, pp. 117–124.

[9] X. T. Cai, F. Z. He, W. D. Li, X. X. Li, and Y. Q. Wu, "Encryption based partial sharing of cad models," *Integrated Computer-Aided Engineering*, vol. 22, pp. 243–260, 2015.

[10] *Cadmatic 3D Outfitting*, Cadmatic, Inc, 2016. [Online]. Available: http://www.cadmatic.com/en/assets/uploads/POD3-%20Outfitting%20Detail%20design%20suite%202015Q3.pdf

[11] Navisworks. (Hämtad: 6.3.2017). [Online]. Available: http://www.autodesk.com/products/navisworks/overview

[12] Microsoft information rights management. Microsoft. (Hämtad: 27.2.2017). [Online]. Available: "https://support.office.com/en-us/article/Information-Rights-Management-in-Office-2010-c7a70797-6b1e-493f-acf7-92a39b85e30c"

[13] Adobe lifecycle es4. Adobe Systems Incorporated. (Hämtad: 14.2.2017). [Online]. Available: "http://www.adobe.com/products/livecycle.html"

[14] Microsoft azure rights management. Microsoft. (Hämtad: 14.2.2017). [Online]. Available: "https://products.office.com/en-us/business/microsoft-azure-rights-management"

[15] Spoofing, idg:s it-ord. IDG.se. (Hämtad: 20.2.2017). [Online]. Available: "https://it-ord.idg.se/ord/spoofing/"

[16] D. Pandya, K. R. Narayan, S. Thakkar, T. Madhekar, and B. Thakare, "An overview of various authentication methods and protocols," *International Journal of Computer Applications*, vol. 131, no. 9, pp. 25–27, December 2015, published by Foundation of Computer Science (FCS), NY, USA.

[17] O. Levillain, A. Ébalard, B. Morin, and H. Debar, "One year of ssl internet measurement," in *Proceedings of the 28th Annual Computer Security Applications Conference*, ser. ACSAC '12. New York, NY, USA: ACM, 2012, pp. 11–20.

[18] M. Georgiev, S. Iyengar, S. Jana, R. Anubhai, D. Boneh, and V. Shmatikov, "The most dangerous code in the world: Validating ssl certificates in non-browser software," in *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, ser. CCS '12. New York, NY, USA: ACM, 2012, pp. 38–49.

[19] D. Florencio and C. Herley, "A large-scale study of web password habits," in *Proceedings of the 16th International Conference on World Wide Web*, ser. WWW '07. New York, NY, USA: ACM, 2007, pp. 657–666. [Online]. Available: http://doi.acm.org/10.1145/1242572.1242661

[20] Adobe photoshop cc. Adobe. (Hämtad: 16.3.2017). [Online]. Available: "http://www.adobe.com/se/products/photoshop.html"

[21] A. Khanse. How does trial software work? The Windows Club. (Hämtad: 16.3.2017). [Online]. Available: "http://www.thewindowsclub.com/how-does-trial-software-version-work"

[22] K. Tevfik, C. Mihai, and I. Rob, "Opening pandora's box: Using binary code rewrite to bypass license checks," 1999.

[23] C. Stanley, E. Philip, J. Harold, and C. V. O. Paul, "White-box cryptography and an aes implementation," *Lecture Notes in Computer Science (LNCS)*, vol. 2596, pp. 250–270, 2002.

[24] W. A. Swee, S. H. J. S. Mariyam, and S. Yahya, "Ship hull fitting using nurbs," *Proceedings of the Computer Graphics, Imaging and Vision: New Trends*, 2005.

[25] Analog hole. Electronic Frontier Foundation. (Hämtad: 21.2.2017). [Online]. Available: "https://www.eff.org/sv/issues/analog-hole"