Undersøgelse af piratdekoderkort m.v.
CENTER FOR TELE-INFORMATION
Apil 1999

Forord

Kulturministeriet anmodede ved skrivelse af 19. november 1998 Center for Tele-Information om for ministeriet at gennemføre en undersøgelse af piratdekoderkort m.v.

Baggrunden for undersøgelsen angives at være, at ændringen af radio- og fjernsynsloven pr.1. januar 1997 gjorde erhvervsmæssige aktiviteter med det formål at give uautoriseret adgang til indholdet af kodede radio- og fjernsyns udsendelser ulovlige, mens privat brug – dvs. eget, personligt brug – af f.eks. piratdekoderkort fortsat ikke er ulovlig. Forskellige rettighedshavere (betalings-tv-stationer, dekoderkortselskaber, kabeloperatører mfl.) har imidlertid påpeget, at dette forhold er uholdbart, og at der er behov for at stramme forbudet op, dvs. også forbyde besiddelse af piratdekoderkort til privat brug.

Nærværende rapport skal dels belyse erfaringerne med den gældende ordning, dels om et sådant strammere forbud vil have den ønskede effekt.

Rapporten er redigeret af centerleder Knud Erik Skouby og følgende medarbejdere har i øvrigt medvirket: BA.polit. Søren C. Jensen, samt de ph.d. studerende cand.scient.pol. Thomas Myrup Kristensen, civ.ing. Reza Tadayoni og civ.ing. Alexander G. Øst.

Lyngby
April 1999

CENTER FOR TELE-INFORMATION
DANMARKS TEKNISKE UNIVERSITET
ELEKTROVEJ, BYGNING 371
2800 LYNGBY
TLF. 4587 1577

FAX. 4596 3171
E-MAIL: CTI@CTI.DTU.DK

Indhold

1. Indledning

Udviklingen inden for broadcasting har indenfor de seneste 10 år været præget af store forandringer både i udlandet og herhjemme. Den traditionelle analoge jordbaserede fremføring af signaler er blevet suppleret med både kabel- og satellitfremføring, og i takt hermed er der fremkommet nye typer af ydelser og tjenesteudbydere. Denne udvikling forventes forstærket af den digitale distributionsteknologi, der er under introduktion i flere Vesteuropæiske lande - herunder Danmark - hvor det sker på forsøgsbasis.

I den analoge, jordbaserede fremføringsteknologi er der frekvensmæssigt kun plads til få landsdækkende tjenester, og muligheden for at udbyde tjenester har i de fleste lande været begrænset til nogle få tjenesteudbydere. Disse har oftest haft eneretten på området mod at optræde som public service broadcastere, der typisk har været forpligtede til at tilgodese en række forhold i udsendelsesudbuddet. Samtidig har finansieringen været baseret på licensbetalinger opgjort efter objektive kriterier (f.eks. at man var indehaver af en modtager), hvad der netop har været begrundet i public service forpligtelsen.

Fremvæksten af mulighederne for at fremføre tv-signaler via kabel eller satellit har sammen med den begyndende digitalisering betydet en kapacitetsudvidelse, der har skabt grundlag for helt nye former for tjenester. Disse øgede muligheder har samtidig medført behov for ændringer i finansieringsmåde og opkrævningskriterier, bl.a. fordi der ikke længere udelukkende er tale om public service aktiviteter, der berettiger brug af hårde, objektive opkrævningskriterier. Udnyttelsen af potentialerne i de nye tjenester beror samtidig på at man kan anvende differentierede priser og finansieringsformer. De nye tekniske muligheder har bl.a. øget mulighederne for at skræddersy specifikke ydelser. Men producenterne af sådanne tjenester kræver i det omfang, der er tale om kommercielle ydelser, typisk også, at betalingen kan skræddersyes, således at kun den, som betaler for en given ydelse, får del i den. Adgangen til at få en bestemt ydelse skal kunne kontrolleres og kunne gøres betinget af betaling. Dette er typisk søgt sikret ved en kombination af kodning af de udsendte signaler og adgangsstyring ved hjælp af såkaldte smart cards.

Den tilsigtede adgangsstyring er blevet omgået ved såkaldte pirataktiviteter, der bl.a. indebærer, at kodningen af radio-/ tv-signalerne brydes eller 'knækkes' og at der fremstilles uautoriserede

dekoderkort, piratkort, som giver adgang til givne tjenester. Det er hovedformålet med denne rapports analyser at afklare, hvilket omfang den uautoriserede adgang har, samt om der kan forventes positive effekter af en stramning af lovgivningen uden for store utilsigtede negative virkninger på andre områder. I analyserne inddrages lovgivningsmæssige erfaringer fra de nordiske lande samt beskrivelser af den tekniske udvikling på kodnings- og adgangsstyringsområdet, herunder den forventede effekt af yderligere digitalisering af disse systemer.

2. Kodningssystemer

De adgangsstyringssystemer man benytter sig af i dag, baserer sig typisk på, at de udsendte signaler udsendes i kodet form, hvorefter de dekodes hos modtageren. Systemerne betegnes som scramblingsystemer, kodnings-/dekodningssystemer eller slet og ret kodningssystemer. Den sidste betegnelse vil blive anvendt i det følgende.

For kabel-tv-udbyderne er piratvirksomhed ikke noget nævneværdigt problem i modsætning til satellitdistribueret tv. Dette skyldes fortrinsvis, at de set-top-bokse, der anvendes i forbindelse med kabel-tv, ikke er beregnet til smartcards. Dekrypteringsmekanismen er indbygget i boksens hardware, og kan kun med vanskelighed reproduceres. Boksene købes samme sted, som abonnementet tegnes, således at tv-udbyderne har et godt overblik over deres abonnenter. I praksis er den eneste måde at blive pirat-tv-kigger på kabelnettet at købe en stjålen set-top-boks eller selv at melde sin boks stjålet - begge måder er indlysende ulovlige og næppe udbredte. Alternativt kan en tilsvarende boks konstrueres med de nødvendige elektroniske komponenter, men dette er kun en teoretisk mulighed, da det ville være et særdeles omfattende projekt - selv for en professionel elektronikmontør.

Fremover kræver betalings-tv via Tele Danmarks kabel-tv-netværk typisk en Selector-boks. Denne boks er digital, og krypteringen af programmerne er derfor forholdsvis sikker, selv om den er baseret på smartcard-teknologi. I lighed med Tele Danmark forventer Stofa fremover at basere deres betalings-tv på et lignende apparat. Det kan derfor forventes, at piratvirksomhed vil forblive et uvæsentligt problem hvad angår kabel-tv.

I de fleste tilfælde bygger systemerne på en kombination af kodning og den såkaldte smart card teknologi. Et smart card gemmer information på en integreret mikroprocessor indfældet i et plastikkort. Grundlæggende findes der to typer smart card. De mest avancerede er de såkaldte intelligente kort, der indeholder en CPU (Central Processing Unit), som både kan gemme og bearbejde information samt udføre operationer i overensstemmelse med de applikationer, kortudstederen har ønsket. De kort, der anvendes i dekoderne, er overvejende af denne type. Herudover findes de såkaldte memory-kort, der primært fungerer som bærere af information, som f.eks forudbetalte telefonkort.

Smart card'ene benævnes også ISO 7816-kort efter den standard, der fastlægger deres funktioner. På kortets overflade er placeret en (guldbelagt) kontaktplade med 8 kontakter, hvoraf de 6 er 'aktive', hvorigennem forbindelsen mellem kort og dekoder skabes. Da ISO-standarden også omfatter kontaktløse kort, hvor interface sker via induktion, kaldes kortene undertiden også for kontaktkort.

Tidligere design af kodningssystemer byggede på det såkaldte 'secure embedded microcontroller' koncept, hvor sikkerhedssystemet var indlejret i signalmodtageren. Smart card teknologien bygger derimod på 'secure detachable microcontroller' konceptet, hvor sikkerhedssystemet er baseret på software, der kan ændres, eller evt. på det integrerede kort, der kan udskiftes, f.eks. hvis systemet brydes gennem 'hack', der betegner uautoriseret brud af systemkoderne. De ældre systemer var sårbare i den forstand at et hack af sikkerhedssystemet – i dette tilfælde af chip'en med systemets koder – betød, at

alle dekodere skulle udskiftes eller opgraderes. Smart card systemerne muliggør en relativ billig udskiftning i tilfælde af hack.

De mest udbredte systemer er i dag endvidere OTA (Over The Air) adresserbare, hvilket betyder, at operatøren centralt kan aktivere og deaktivere den tilmeldte abonnents dekoder f.eks. i henhold til betaling eller ikke-betaling. I ældre systemer eksisterede den mulighed ikke, men denne nye mulighed betyder imidlertid generelt ikke, at man centralt kan styre eller afbryde adgang for ikke-autoriserede kort (piratkort).

2.1 ANALOGE OG DIGITALE SYSTEMER

Hovedparten af de eksisterende systemer har deres oprindelse i analog teknologi, idet signalerne transmitteres i et analogt format. De tidlige kodningssystemer var helt igennem analoge og kodningen bestod blot i simple manipulationer af signalerne (ændringer af sync pulsene eller enkle ombytninger af fjernsynslinier). Denne kodning var relativ let at bryde og systemerne var således meget sårbare overfor uautoriseret adgang og ydede lille beskyttelse for operatørerne, idet det også var relativt enkelt at fremstille dekodere, der fungerede på samme måde som de autoriserede.

De mest udbredte systemer i Europa i dag er VideoCrypt (i forbindelse med transmissionsstandarderne PAL og NICAM), EuroCrypt (i forbindelse med D2-MAC) og Nagravison. Disse systemer har gennem smart cards introduceret digital teknologi til beskyttelse af den analoge signaltransmission. EuroCrypt er den udbredte standard i Norden, idet den anvendes af både FilmNet, TV 1000, TV3, Canal Plus (i den såkaldte EuroCrypt-M form) og Canal Digital (i EuroCrypt-S formen). VideoCrypt har stor udbre-delse i Storbritannien, hvor den blandt andet anvendes af BskyB, mens Nagravision er udbredt i Frankrig, Spanien og Tyskland. I modsætning til de bokse, der følger VideoCrypt og EuroCrypt standarderne, er Nagravision dekoderboksene ikke til salg, men lejes ud til abonnenterne.

Bortset fra Nagavision-dekodere, er det sædvanligt, at brugeren selv anskaffer sin satellitmodtager. De fleste af disse er udstyret med en integreret dekoderenhed, herunder kortlæser. Når systemet modtager et signal aflæses signalet for kanal-specifikke oplysninger, herunder sikkerhedskoder. Ukodede signaler sendes uden om dekodnings-enheden, medens kodede signaler/ programmer sendes gennem dekoderenheden. De aflæste informationer bearbejdes af kortlæseren og kombineres med kort-informationerne, hvorefter dekodningsenheden aktiveres, i den udstrækning kortet er programmeret til det - f.eks. hvis indehaveren af kortet har betalt for en bestemt kanal. Kortet kan som udgangspunkt anvendes på en hvilken som helst kortlæser, indehaveren måtte ønske forudsat at satellitmodtageren understøtter standarden, men i flere systemer indeholder kortet/ signalet en kode, der første gang kortet anvendes, binder det til den pågældende modtager.

Den måde det udsendte signal er kodet og hvorledes modtageren efterfølgende afkoder det, er bestemt af den gældende kodningsstandard. I den dominerende standard for transmission af satellitsignaler i Norden (den såkaldte D2-MAC standard) anvendes EuroCrypt-standarden. Modtageren må for at være i stand til at modtage afkodede signaler på den enkelte fjernsynsskærm derfor være i besiddelse af en IRD (Integrated Receiver Decoder) der er kompatibel med denne standard. De fleste kendte elektronik-fabrikater leverer modtagere i denne standard.

Kodningen består i en manipulering af det 'originale' signal, hvorefter der hos modtageren sker en genskabelse af det originale signal i IRD's dekoderdel.

Kodningen er imidlertid blot en af komponenterne i det komplicerede tekniske og administrative adgangsstyringssystem der holder rede på og giver adgang for brugere, der har købt adgang til bestemte

services (som f.eks pay-TV). Kodningen af signalet sker på basis af et såkaldt Code Word (CW) der styrer den konkrete kodning. Dette CW krypteres og sendes sammen med det kodede satellitsignal til modtageren. Det krypterede CW betegnes som operationskoden, og afkrypteringsmekanismen går under betegnelsen management key. Herudover findes også en såkaldt adresse- eller zonekode, der angiver hvilket selskab signalet stammer fra.

Hos modtageren sker der en bearbejdning af det krypterede CW. Bearbejdning udføres af det smart card der af abonnenten er indlæst i IRD's kortlæser. Kortet er i stand til at dekryptere koden og på basis heraf sikre at det kodede satellitsignal afkodes, selvfølgelig under forudsætning af at kunden abonnerer på den pågældende service.

Smart card'et udsendes til de enkelte abonnementer i forbindelse med tegning af abonnement. Når abonnementet ophører forventes abonnenten at tilbagesende smart card'et til serviceudbyderen, idet systemet er baseret på at abonnenten lejer kortet.

Det er operationskoderne, som piraterne offentliggør under betegnelsen D2-Mac-koder på deres hjemmesider på Internet og lignende steder. Der er ingen tvivl om at denne offentliggørelsesmåde har reduceret effektiviteten i selskabernes adgangsstyrings-systemer, jfr. nedenfor.

Det tager tid at opdatere operationskoderne. Det hænger til dels sammen med at systemet er gammelt. Men også at selskaberne må være sikre på at deres kunder faktisk får opdateret kortene. Hvis kortet ikke sidder i kortlæseren kan det ikke opdateres og derfor ikke modtage den nye operationskode. Opdateringen må derfor foregå i en så tilpas udstrakt periode at selskaberne er sikre på at alle deres kunder har fået deres kort opdateret. I modsat fald risikerer selskaberne at nogle kunder ikke får opdateret deres kort, hvilket i bedste fald vil skabe irritation hos kunden. Den tid der går mellem opdateringer er derfor en afvejning selskaberne må gøre mellem på den ene side hvor vanskeligt de vil gøre livet for piraterne og på den anden side de forskellige problemer der kan opstå hos deres kunder. Problemet accentueres af at det ikke er de samme management keys der er knyttet til alle kundekortene, hvorfor selskaberne, hver gang der skal foretages omkodninger, er nødsaget til at gennemføre en rutine for at sikre sig at alle de forskellige kort er opdaterede. At CanalDigital har et langt kortere interval mellem sine opdateringer (hver 2-3 dag) end Viasat (hver 2-3 uge) hænger sammen med at Canal Digital har et langt mindre kundegrundlag og at den variant at kodningsstandarden CanalDigital anvender (nemlig EuroCrypt-S) er nemmere at arbejde med.

Det er den relativt lange tid mellem opdateringerne der giver hackere mulighed for at nå at finde og offentliggøre nye koder og for piraterne at udnytte dem.

Ingen af selskaberne synes – i modsætning til hvad der er tilfældet hos f.eks. de britiske selskab BskyB - i nogen større grad at have anvendt kortudskiftning i deres kamp mod piraterne. Sidst Canal Digital udskiftede sit kort var i foråret 1997, netop i forbindelse med selskabets overgang fra EuroCrypt-M til EuroCrypt-S.

At det forholder sig sådan hænger formentlig sammen med at det grundlæggende hack bag udbredelsen af piratdekoderkortene ligger i hackningen af EuroCrypt standarden, mere end det ligger i hackningen af koder (det er hacket af standarden der muliggør at piraterne kan hacke operationskoderne). Hertil kommer at en kortudskiftning opfattes som en dyr affære for selskaberne. F.eks. vil alene indkøbet af kort koste Viasat i omegnen af 30 mio. kroner. Og som sagt er udsigterne for på denne måde at komme piraterriet til livs ikke særlige lyse, på grund af 'miljøets' kendskab til kodningsstandarden. En udskiftning af kodningsstandarden vil kræve at kunderne må udskifte deres receivere.

De kort selskaberne anvender er som sagt baseret på den såkaldte smart card teknologi. Det vil sige at der er tale om en standard, og selskaberne anvender flere leverandører af disse kort. På den ene side har selskaberne af sikkerhedshensyn måske nok haft et ønske om kun at have én leverandør (fordi lækager i sikkerheden potentielt dermed mindskes), men omvendt har det vist sig vanskeligt at finde en og samme leverandør der er i stand til at levere så mange kort som der er behov for.

Et fuldt digitalt distributionssystem betyder, at kodningen kan blive mere kompliceret, men også at opdateringen af koder kan ske langt oftere uden gener for abonnenterne. På det tekniske plan betyder digitaliseringen at 'kodningskapaciteten' kan sættes i vejret, dels ved en forøgelse i frekvensen af kodningsrelateret information, dels ved at kodningen bliver mere kompleks (f.eks. kan kodningen finde sted på hvert enkelt af TV-billedets punkter, hvor det i dag sker der en kodning af enten det enkelte billede (frames), billedets enkelte linier eller Croma og Luminans).

Også på det 'administrative' plan vil digitaliseringen formentlig øge effektiviteten i kodningen (adgangsstyringen), således at der oftere kan gennemføres ændringer i kodningen uden efterfølgende gener for abonnenterne. Den afvejning selskabernes hele tiden må foretage mellem på den ene side de gener et givet kodningssystem skaber for kunderne og på den anden side de 'vanskeligheder' det skaber for pirater ændres altså ikke ved overgang til et digitalt system, men digitaliseringen gør det muligt at øge vanskelighederne for de sidstnævnte til fastholdt gene for de førstnævnte (se kapitel nedenfor vedrørende digitale systemer).

3. Piratkort

Piratkort er den populære betegnelse for ikke-autoriserede smart cards, der er i stand til at afkode kodede tv-signaler. Anvendelse til afkodning kræver, at kortene programmeres til dette. De eksisterende kort er enten for-programmerede, eller 'tomme' / blanke. De sidstnævnte skal programmeres inden brug ved hjælp af en kortbrænder, der er et forholdsvis simpelt stykke elektronik, der tilsluttes en pc (se bilag 1). De relevante koder lægges herefter ind på kortet ved hjælp af software. Den software der skal bruges i forbin-delse med programmeringen af kortet, kan findes på Internettet som free-ware, ligesom de nødvendige koder - der er kanalafhængige - også forholdsvis let findes på Internettet.

Piratkort findes tillige som print-kort bestykket med mikroprocessorer og andre elektroniske dele. Printkortene fungerer som smart cards, men er en smule mere klodsede blandt andet fordi chips'en 'stikker ud' fra printpladen og fordi pladen ikke på samme måde som smart cards kan placeres inde i kortlæsere.

Nogle programmer til indlægning af koder på smart card giver mulighed for, at fjernkontrollen til satellitmodtageren kan anvendes til at indtaste opdaterede koder, som kan hentes fra Internettet. Andre kort kræver dog indtastning via pc.

Der er tre former for kode, der lægges ind på kortene:

- Adressekode
- Hemmelig bagkode (også kaldet "management key")
- Operationskode

De to førstnævnte koder ligger på de autoriserede kort og knytter bl.a. kortet til et bestemt apparat. Operationskoden er den, der anvendes af piratkiggerne og som findes på Internettet. Hvis det kommer

til udbyderens kendskab, at en management key er blevet hacket og er i omløb, vil den blive lukket. Nødvendigheden af til stadighed 'manuelt' at skulle opdatere operationskoderne i piratkortene (og at dette altså ikke kan ske automatisk 'via luften', som det er tilfældet med de autoriserede kort) hænger netop sammen med, at piratkortene ikke er forsynet med disse management keys.

Ifølge David Würgler (organisationen STOP) er langt de fleste piratkort i omløb af den type, der opdateres mauelt.

Den overvejende del af piratkortene er baseret på Microchips' PIC16C84 eller PIC16F84 processorer (men også f.eks. Dallas DS5002 bruges), hvorfor kortbrænderen også benævnes PIC-brænder. De simpleste piratkort er de såkaldte 1-pic kort, der består af en enkelt PIC16F84 chip. Kapaciteten i disse kort er imidlertid begrænset, således at der skal bruges ét kort for hver kanal (for at kunne se både CanalDigital og ViaSat skal man således have 2 kort, idet CanalDigital anvender EuroCrypt-S, medens ViaSat benytter sig af EuroCrypt-M).

Et såkaldt MultiMac 2 kort består af en 16F84 chip samt en 24LC16 eeprom. Eeprom'en, der er en lagringsenhed, hvis indhold kan slettes elektronisk, giver samtidig plads til flere koder end standardkortet (1-pic kortet), og det er derfor kun nødvendigt med ét kort for at se alle kanaler, der generelt opfattes som relevante i Danmark. Kortet fungerer angiveligt på de fleste modtagere. Prisen for et tomt MultiMac 2 kort er i størrelsesordenen 100 kr., medens en brænder kan erhverves for 155 kr.

Uautoriseret adgang til det beskyttede programs udbud kræver, at sikkerhedssystemerne er blevet hacket. Der eksisterer imidlertid forskellige måder, hvorpå dette finder sted og det kan være værd at notere at piratkort blot er en blandt flere metoder til uautoriseret adgang til at se de beskyttede kanalers udbud.

I dele af hackermiljøet taler man f.eks. om det såkaldte grey market card, som betegner kort hvor indehaveren betaler et abonnement, men ikke bor i et område, hvor der lovligt er adgang til kanalen.

Phoenix-kort er betegnelsen for originale kort, der uautoriseret bliver reaktiveret. Et kendt eksempel på dette er Phoenix Sky 9 kort, der er en reaktivering af den britiske serviceprovider BSkyB's 9. generation af kort, idet BSkyB løbende har fornyet kortene for at imødegå hack'ing samt indlagre teknologisk fornyelse.

En anden kendt metode til at skaffe sig adgang til specifikke programmer er udnyttelse af det såkaldte Season interface software i forbindelse med såkaldte VCL-filer. Program-merne ses ved denne metode dog ikke i realtid, idet de først optages på video-optager i kodet form. VCL-filerne som hentes fra Internettet er rene afkodnings-programmer, der afkoder specifikke udsendelser sendt på specifikke tidspunkter. Ved hjælp af Season-programmet og VCL-filerne er det muligt at dekode de signaler, som er hentet ned på video-optageren.

Såvidt det har kunnet konstateres, findes der for tiden kun VCL-filer til programmer sendt af BSkyB. Det forlyder i øvrigt, at den første pay-per-view-udsendelse, som BSkyB gennemførte blev hacket på denne måde. Da BSkyB samtidig genudsendte programmet over en periode på en uge var det oven i købet muligt at se det i real-tid.

Opsummerende kan det således konstateres, at der findes en række muligheder for at skaffe sig uautoriseret adgang til beskyttede radio-/ tv-programmer, at de er relativt lette at erhverve, og at de

findes i brugervenlige udgaver, således at anvendelse ikke kræver teknisk indsigt. Det sidstnævnte forhold kræver dog, at 'nogen' fremstiller de uautoriserede kort med henblik på uautoriseret radio-/tv-adagng til beskyttede systemer. Det må derfor antages, at langt den overvejende del af piratdekoderkort på markedet er købt med management key fra en piratkort-sælger.

4. Lovgrundlaget i Danmark, EU og Norden

4.1 DET GENERELLE LOVGRUNDLAG

Tre love har betydning for området vedrørende uautoriseret dekodning af radio-/ tv-signaler i Danmark:

Lov om radio og fjernsynsvirksomhed – der regulerer de centrale forhold vedrørende adgang til radio og tv signaler.

Ophavsretslovgivningen – forbyder kopiering, men dekodning af tv signaler betragtes ikke som kopiering sålænge signalet ikke lagres.

Markedsføringsloven – forbyder dårlig salgsskik/moral. Salg af piratkort mm. kan betragtes som dårlig markedsføringsskik.

Hertil kommer en række internationale konventioner, samt et EU-direktiv.

4.2 LOV OM RADIO- OG FJERNSYNSVIRKSOMHED

Folketinget vedtog d. 29. december 1997 lov nr. 1095 som forbyder fremstilling, markedsføring, overdragelse, udlejning, installation og vedligeholdelse af udstyr, der uautoriseret giver adgang til indholdet af en kodet radio- eller tv-udsendelse. Loven trådte i kraft d. 1. januar 1998. Loven omfatter dekodere såvel som andet dekodningsudstyr som programkort, der kan anvendes med samme formål som en dekoder. Loven gør al erhvervsmæssig virksomhed i forbindelse med tv-pirateri ulovlig, mens privat fremstilling, besiddelse og brug af piratkort ikke er omfattet af forbudet. Loven fortolkes herudover således, at der kræves forsæt eller grov uagtsomhed for at falde ind under forbudet. Grænsen mellem private og erhvervsmæssige forhold er i bemærkningerne til loven fastsat således, at en privatpersons enkeltstående videresalg af en piratdekoder, som vedkommende ikke længere ønsker at benytte, ikke betragtes som ulovligt.

Det er alene anklagemyndigheden der har kompetence til at rejse sager efter loven (§2). Forurettede rettighedshavere kan ikke rejse krav om strafansvar, men er henvist til et civilretsligt erstatningskrav. Ved en kodet radio- eller tv-udsendelse forstås en udsendelse, hvis signal i form af lyd og/eller billede er forvrænget med det formål, at kun modtagere, der anskaffer et individuelt eller kollektivt abonnement hos programleverandøren eller dekoderselskabet, kan få adgang til indholdet af udsendelserne[1]. Udtrykket kodning kan derfor betragtes som et synonym for kryptering.

Strafferammen for overtrædelse er fastsat til op til seks måneders fængsel, en straf der sandsynligvis først benyttes i gentagelsestilfælde. Førstegangsovertrædelse vil antageligt blive straffet med bøde. Der er hidtil ikke blevet foretaget domfældelse af pirater i Danmark efter denne lovgivning.

4.3 EU REGULERING

Siden 1996 har Kommissionen, Rådet og parlamentet arbejdet med et forslag til et direktiv om retlig beskyttelse af adgangsstyrede og adgangsstyrende tjenester. Direktivet 98/84/EF blev vedtaget d. 28. november 1999 og medlemsstaterne skal efterkomme direktivet senest d. 28. maj 2000.

Direktivet indeholder udelukkende et forbud mod kommerciel piratvirksomhed og omfatter således ikke privat brug eller omsætning af piratkort mm. Direktivet fastlægger dog kun et minimumsniveau for regulering, således at det er muligt for enkeltstaterne at gå videre end de regler, som direktivet fastsætter. Handlinger som medlemsstaterne opfordres til at tage hvis det skønnes nødvendigt.

Dog er der i forbindelse med EU-direktivets tilbliven opstået en diskussion om, hvorvidt den passage i direktivet, som omhandler et forbud mod kommunikation med henblik på at fremme udbredelsen af ulovlige anordninger (art. 4. c) der kan ses som et de facto forbud mod piratdekodning af kodede radio- og tv-signaler[2]. Det skyldes at de fleste piratkort kræver manuel opdatering af koderne efterhånden som broadcasteren ændrer disse (jf. foregående kapitel). Denne manuelle opdatering er afhænging af at opdateringskoderne udsendes til pirattv-seerne. Denne udsendelse foregår som oftest ved hjælp af e-mail eller såkaldte SMS-beskeder der udsendes på mobiltelefon nettet.

Direktivet nævner dog, at der er tale om kommerciel kommunikation, så om en sådan fortolkning af direktivet er holdbar, må sandsynligvis komme an på en domstolsafprøvelse.

4.4 REGULERING I SVERIGE

Den svenske regulering er i høj grad på linie med den nuværende danske lovgivning. Det skyldes ikke mindst at den danske lov er udarbejdet med inspiration fra den svenske[3].

Således forbyder en svensk lov fra 1993 fremstilling, overdragelse, udlejning, installation og vedligeholdelse af uautoriseret dekoderudstyr. Loven omfatter, ligesom det er tilfældet i Danmark, kun forhold af erhvervsmæssig karakter. Det er ikke ulovligt at benytte uautoriserede kort i Sverige.

Der arbejdes på at tilpasse den svenske lov til EU regulativet. Dette vil også føre til en revurdering af hvorvidt brug af uautoriserede piratdekoderkort skal gøres ulovlig.

4.5 REGULERING I NORGE

Norge foretog i 1995 en stramning af lovgivningen således at både salg af og besiddelse, inklusiv privat brug af piratkort blev forbudt. I modsætning til Danmark og Sverige hvor piratdekoderproblematikken reguleres gennem en særlov, reguleres området i Norge ved hjælp af den norske straffelovs §262, der forbyder salg, privat brug og besiddelse af udstyr der kan benyttes til uautoriseret dekodning af tv- og radiosignaler.

Strafferammen i Norge er væsentlig højere end i de to andre skandinaviske lande. På den erhvervsmæssige side blev en 40 årig mand i 1997 således idømt et års fængsel samt en bøde på 1.885.000 NOK for ulovlig fremstilling og videresalg af piratdekoderkort. På privatbrugersiden er over 1.000 piratseere i en enkelt sag blevet mødt med bøder på 5.000 NOK for brugen af uautoriserede dekoderkort.

Som i Danmark og Sverige betragtes salget af piratdekoderkort mm. i Norge desuden som en overtrædelse af markedsføringslovens §1 om god markedsføringsskik.

Der er så vidt vides ingen planer om at ændre den norske lovgivning på piratdekoder-området.

	Danmark	Sverige	Norge	EU

	Reguleret af	Lovnr. 1095 af 29.dec. 1997 forbyder fremstilling, markedsføring og salg af piratkort	Lag (1993:1367) forbyder fremstilling, overdragelse, udlejning, installation eller vedligeholdelse i erhvervsmæssigt øjemed	Norske straffelov §262. Salg, privat brug og besiddelse betragtes som underslæb og tyveri	KOM (98) 332 & Rådets direktiv om retlig beskyttelse af adgangsstyrede og adgangsstyrende tjenester 98/84/EF af 20. nov. 1999
Ud-buds-siden	Strafferamme	I første gangs tilfælde bøde, men strafferamme på 6 måneders fængsel	Bøde. Strafferamme på seks måneders fængsel	Bøde eller fængsel op til et år.	
	Erhvervsmæssig fremstilling og salg	Ulovligt	Ulovligt	Ulovligt	Ulovligt
	Privat fremstilling	Lovligt	Lovligt	Ulovligt	Lovligt, medlemslandene kan gå videre
	Køb og salg af blanke smart-cards/ programkort	Lovligt	Lovligt	Lovligt	Lovligt, medlemslandene kan gå videre
	Sager	Selskaberne får nedlagt fogedforbud mod piratsælgere.		Storpirat idømt 8 måneders fængsel + 1.9 mio. NOK i bøde i 98	
Efter-spørg-sel	Benyttelse af piratkort	Lovligt	Lovligt	Ulovligt	Lovligt, men opdatering måske ulovlig[4]. Medlemslandene kan gå videre
	Strafferamme	-	-	Bøde ca. 5.000 NOK	
	Sager	-	-	1000 piratseere blev med hjælp fra udbyderene tilsendt bødeforlæg opfulgt af retssager i 1995	-

5. Hvor stort er pirat-tv-problemet i Danmark?

5.1 INDLEDNING

Dette kapitel har til formål at skabe et overblik over hvor stort pirat-tv-problemet er i Danmark. Dvs. give et overblik over hvor mange, der uautoriseret ser kodede tv-programmer. En sådan opgørelse er imidlertid forbundet med betydelige problemer. Det viser sig bl.a. andet ved det forhold, at mange mener, at pirat-tv, på trods af det ikke er ulovligt, er en aktivitet, der befinder sig i en moralsk gråzone,

som man som følge heraf ikke er særlig villig til - ærligt - at oplyse om.

5.2 VILSTRUP-UNDERSØGELSERNE
I 1997 og juni 1998 fik betalings-tvselskaberne meningsmålingsinstituttet Vilstrup Research til at undersøge, hvor udbredt pirattv-kiggeri er i Danmark. Undersøgelsen er den mest omfattende kortlægning af piratkortenes udbredelse, men er samtidig behæftet med metodiske problemer, således at dens resultater må tages med visse forbehold. Disse består – foruden problemer med at spørge folk om deres deltagelse i aktiviteter, som betragtes som forkerte eller umoralske – i en noget upræcis spørgsmålsformulering, der ikke giver mulighed for en helt præcis skelnen mellem autoriserede seere og pirater.

Denne problematik hænger sammen med det forhold, at det ikke er helt enkelt at definere en pirat. F.eks. medfører betalings-tv-selskabernes hyppige kodeskift, at det må antages, at en betydelig del af de mennesker, der har anskaffet sig uautoriserede dekoderkort er ude af stand til at se de kodede udsendelser, indtil de igen bliver forsynet med de nødvendige kodeopdateringer.

Med disse forbehold giver undersøgelsen et billede af problematikken, der stemmer relativt godt med de bud, der fra forskellig side er fremkommet om størrelsen af den uautoriserede adgang til betalings-tv-kanaler.

5.2.1 Betalings-tv-selskabernes opgørelse
Betalings-tv-selskaberne har benyttet Vilstrup-undersøgelserne til at beregne, at henholdsvis 37% (1997) og 49% (1998) har købt deres dekoderkort på uautoriseret vis, og at henholdsvis 97% (1997) og 99% (1998) af de der ser betalings-tv, får opdateret deres kort på uautoriseret vis.

Ifølge betalings-tv-selskaberne udgør piraterne således en alt dominerende andel af de mennesker, som ser betalings-tv, men disse tal overvurderer efter vores opfattelse problemet. Det anskueliggøres bl.a. af en alternativ opgørelse, som CTI har foretaget på det samme talmateriale.

5.2.2 CTI's opgørelse
Vilstrup-undersøgelsen giver mulighed for at belyse, om folk er i besiddelse af det nødvendige udstyr til at opnå uautoriseret adgang til betalings-tv. Disse tal fremgår af den opgørelse CTI har lavet på baggrund af undersøgelsen (tabel 1). I CTI's opgørelse er Vilstrup-undersøgelsens tal om disse forhold blevet generaliseret til antallet af hustande i Danmark, samt til hele befolkningen.

Det skal bemærkes at denne generalisering behæfter tallene med den sædvanlige statistiske usikkerhed, der dog, i dette tilfælde, må betragtes som ubetydelig set i forhold til andre fejlkilder, som stammer fra emnets og spørgsmålenes karakter.

Tabel 1

	Sample juni 1998		Generaliseret til -->	Personer	Husstande
	%	Antal			
Befolkningen/stikprøven/husstande	100	1.254		5.294.860	2.407.010
Som har kabel eller parabol	72	903		3.812.299	1.733.047
Af ovenstående som har dekoder1	24	217		914.952	415.931

- Herudaf m. betal.tv abbonnement2	53	113	475.416	216.121
- Herudaf m. uautoriseret afgang2	49	104	439.536	199.810

[1] Spørgsmålet antages at dække folk, der har en dekoder med slot til dekoderkort, selv om spørgsmålet er formuleret således, at der spørges om man "har en dekoder".
[2] Grundet afrundingsfejl summerer % til 102.
Befolkningstal og husstande pr. 1. januar 1998 (Statistisk Årbog 1998)

Efter denne opgørelsesmetode er det således ca. halvdelen af de husstande, der ser betalings-tv, der benytter en uautoriseret adgangsform. Dette betyder, at der i juni 1998 var knap 200.000 husstande, der havde uautoriseret adgang til betalings-tv-kanalerne i Danmark. Det svarer til 8.3% af det samlede antal danske husstande.

Lægges de to Vilstrup-undersøgelser til grund, må det konkluderes, at antallet af seere med uautoriseret adgang er stigende. Mens forholdet mellem autoriserede og uautoriserede seere ifølge 1997-undersøgelsen var ca. to til en, er det i 1998 undersøgelsen steget til knap én til én. Endvidere var andelen af husstande med uautoriseret adgang i 1997 ca. 5.6% (Svarende til ca. 135.000 husstande).

5.3 PIRAT-TV PROBLEMETS STØRRELSE
Den af betalings-tv-kanalerne bestilte Vilstrup analyse udgør det mest håndgribelige bevis på pirat-tv's udbredelse i Danmark. Undersøgelsen er dog behæftet med væsentlige usikkerhedsmomenter der gør at dens resultater må tages med betydelige forbehold.

Undersøgelsen viser, ifølge CTI's opgørelse, at der i juni 1998 var omkring 200.000 pirat-tv husstande i Danmark. Dette tal udgør mere end 8% af det samlede antal husstande i Danmark.

Disse tal viser endvidere at forholdet mellem pirater og abonnenter hos betalingsselskaberne er ca. én til én. Betalings-tv-kanalernes påstand om at 99% af deres seere er pirater er således ikke et realistisk tal.

Til gengæld stemmer opgørelsen af antallet af pirater helt overens med betalings-tvselskabernes opgørelse foretaget ved at undersøge antallet af hjemmesidebesøg på sider der stiller opdateringskoder til piratkortene til rådighed. Her nås der i overensstemmelse med CTI's beregninger frem til ca. 200.000 pirater.

6. De danske satellitudbyderes stilling

De to dominerende satellitudbydere i Danmark - Canal Digital og ViaSat - er begge aktive i bekæmpelsen af piratkiggeri. På trods af, at Canal Digital og ViaSat er hinandens største konkurrenter, har de gennem organisationen STOP et fælles talerør[5].

I det følgende gælder de anførte oplysninger Canal Digital såvel som ViaSat, med mindre andet er anført.

Canal Digital skifter operationskode ca. hver 2. eller 3. dag. ViaSat skifter hver 2. eller 3. uge. Det angives at være teknisk meget vanskeligt at skifte kode oftere. Hyppigere kodeskift (f.eks. hvert minut) ville ellers gøre det mindre attraktivt at være piratkigger, da det ville medføre nærmest konstant indtastning af nye koder

6.1 AKTØRERNE

6.1.1 Canal Digital

Canal Digital har en serie forskellige programpakker indeholdende film, underholdning, sport, dokumentarprogrammer og direkte nyheder. Canal Digitals programpakker distribueres gennem et landsdækkende net af autoriserede forhandlere med over 300 radio/tv-forhandlere. Den daglige servicering af nye og gamle kunder står Canal Digitals kundeservice for. Omkring 80 medarbejdere sælger, servicerer og distribuerer Canal Digitals programpakker til parabol.

Canal Digital Danmark er et datterselskab af CANAL+ og Telenor. Telenor er det førende telekommunikationsselskab i Norge og den tredjestørste satellitoperatør i Europa. Antallet af medarbejdere er ca. 3000, heraf ca. 200 i Norden og 80 i Danmark. Antallet af abonnenter var med udgangen af 1997 ca. 10,5 million. CANAL+ er børsnoteret i Paris og er Europas største koncern indenfor betalings-tv, med et nettoresultat i 1996 på ca. 750 millioner FRF.

6.1.2 ViaSat

ViaSat A/S ejes af Modern Times Group, som er en skandinavisk mediekoncern, der er noteret på Nasdaq-børsen i New York og på Stockholms Børsinformation (SBI-listen). Omkring en million skandinaviske husstande - heraf 300.000 danske - er kunder hos ViaSat. Ved udgangen af 1998 fandtes 30 kanaler på ViaSats parabolkort. Udlejning af parabolkort og salg af betalings-tv sker gennem radio- og tv-forhandlere i Danmark samt gennem ViaSats egen kundeservice. ViaSat har omkring 25 ansatte i Danmark.

I modsætning til Canal Digital har ViaSat ingen planer om at sende digitalt. De mener, at merværdien ved digitalt satellit-tv ikke opvejes af ulemperne. Med 300.000 analoge parabolkunder i Danmark vurderer ViaSat, at udgifterne ved udskiftning af det analoge modtageudstyr på nuværende tidspunkt ikke kan betale sig.

6.2 SATELLITUDBYDERNES SYN PÅ PIRATPROBLEMET

Der skal ifølge STOP tre ting til for at løse problemet omkring piratkiggeri[6]:

- Risiko for opdagelse.
- Det skal være mere vanskeligt at være pirat.
- Der skal være større konsekvens mht. straf.

Sædvanligvis bliver der kun nedlagt fogedforbud mod piratkortdistributørerne, der herefter fortsætter deres virksomhed.

Der angives desuden at være behov for at gøre bevissikring mere effektiv (f.eks. ved at det bliver muligt at undersøge piratkortdistributørernes computere for kundekartoteker m.v.), og endelig mener man ikke, at digitalisering løser noget problem.

Der angives at være en risiko for, at filmselskaberne lukker for levering af film (som det skete for TV1000 for nogle år siden) hvis piratkiggeriet er for udbredt. Det skal i denne forbindelse bemærkes, Canal Digital og ViaSat betaler royalties til filmselskaberne baseret på antal abonnenter - de betaler altså ikke for piraterne.

7. Digitalisering og piratkopi-problemet

En af de centrale problemstillinger i udviklingen af digital tv (og i mindre omfang digital radio) har

været håndteringen af sikkerhedssystemer i forbindelse med adgangsstyring. Digitaliseringen af tv skaber bl.a. mulighed for transmission af flere og mere varierende tv services, herunder interaktive services. Dette vil i stadig højere grad blive brugt af kommercielle serviceudbydere herunder operatører af betalings-tv-services. Da nogle betalings-tv-operatører udbyder services fuldstændig fri for reklamer er deres eksistens direkte forbundet med deres indtjening i form af brugerbetaling. Derfor kan evt. brud i adgangsstyringens sikkerhedssystem (hack'ing) have vidtrækkende konsekvenser for disse aktører.

Digitale adgangsstyringsystemer er mere robuste mod hack'ing end de nuværende systemer anvendt i analog TV. Alligevel indrømmer selv de centrale aktører indenfor digital tv, som f.eks. DVB organisationen at de digitale systemer ikke er 100% sikre og at muligheden for hacking / pirateri også eksisterer i den digitale tidsalder. Dette bliver dog utvivlsomt meget mere kompliceret og det er meget svært at være piratkigger når digital teknologi bliver anvendt. Som det fremgår af det følgende bliver der både i standardiseringsarbejdet og i administration af information gjort meget for at reducere piraternes muligheder.

I det følgende gives der en kort gennemgang af adgangsstyringen i den digitale transmission. Senere testes enkelte dele af adgangsstyringsystemet for mulighed for hacking. Dette er på ingen måde et forsøg på at afdække alle dele af access systemer i digital tv[7] men er et forsøg på at beskrive nogle centrale dele for på denne måde at give en bedre forståelse af problemstillingen.

7.1 ADGANGSSTYRING I DEN DIGITALE TRANSMISSION

For at begrænse adgangen til udvalgte tv- services til brugere, som abonnerer på servicen etableres der et adgangsstyringssystem, som krypterer signalet ved udsendelsen på en sådan måde at kun brugere, som har erhvervet sig det nødvendige hardware og/eller software til at afkryptere signalet kan have adgang til servicen.

Adgangsstyringssystemet er et kompliceret teknisk og administrativt system, som holder rede på og giver adgang til brugere, der har ret til udvalgte services herunder "pay per view" services og mere eller mindre sofistikerede data services. På figur 1 (se s. 21) er der givet et meget simplificeret diagram over hvordan krypteringen foregår ved afsenderen.

7.1.1 Adgangsstyring hos udbyderen

Som det fremgår af figur 1 kommer det signal, der skal sendes i distributionsnetværket først igennem en signalbehandling, som sørger for at signalet bliver uigenkendeligt. Senere genskabes signalet af systemet på modtagesiden (se figur 2). I det følgende beskrives figur 1 mere detaljeret.

Den indkommende datastrøm (på figuren) kan f.eks. være en tv-service, som skal sendes til bruger 1. Tv signalet har altså været digitaliseret, komprimeret mm. og på dette tidspunkt er det således en række tal (data 1 .. data n) der skal videresendes. For at gøre dataværdierne uigenkendelige skal disse talværdier igennem et modul som teknisk hedder en "scrambler".

Scrambleren består af en pseudo-tilfældig tal-generator, som genererer en sekvens af tilfældige tal (tal 1 .. tal n på figuren). Denne talsekvens kan senere genskabes og heraf navnet psuedo-tilfældig. En matematisk operation udføres mellem tal 1 og data 1, tal 2 og data 2 …tal n og data n. Resultatet bliver data 1' .. data n', som sendes i distributions netværket.

Lad os f.eks.antage at den matematiske operation er summation. Altså data 1' = tal 1 + data 1, data 2' = tal 2 + data 2 mm. Senere ved modtagelsen gen-genereres tal1 .. tal n. Disse trækkes fra data 1' .. data n' og på denne måde genskabes data1 .. data n.

Den algoritme, som generer talsekvensen tal 1 .. tal n er yderst beskyttet af standardiseringsorganerne og afleveres kun til producenterne under strenge "None Disclose" aftaler.

For at gøre det endnu mere vanskeligt at bryde algoritmen afhænger talsekvensen tal 1 .. tal n af et kodeord (Code Word, CW i figuren), som genereres af CA systemet. Dette betyder at selv når scrambling algoritmen er brudt, er man stadig nødt til at kende CW for at genere talsekvensen. Forskellige CA-system-udbydere anvender forskellige meget hemmeligholdte algoritmer for at genere CW og de skifter CW meget hyppigt f.eks. hver 8. sekund. CW kan i princippet generes af en (rigtig) tilfældig-tal-generator. Altså en tilfældig-tal-generator, som kan generere en talsekvens, som aldrig kan genskabes[8] selvom man har en tro kopi af generatoren. CW bliver krypteret og sendt sammen med data til modtageren, således at modtageapparatet har mulighed for at afkode signalet.

CA systemet har et kontrolmodul, som håndterer selve abonnent styringen og f.eks. styrer hvilke af de indkommende data, der skal" scrambles". For eksempel skal "free to air" services (herunder f.eks. public service og nogle reklame baserede services) ikke scrambles da de skal være frit tilgængelige for alle. Dette er på figur 1 afbildet med en pil fra kontrolmodulet til modulet med matematisk operation. Kontrolmodulet signalerer således til den matematiske operation om at holde op med operationen når f.eks. "free to air" data skal passere.

7.1.2 Adgangsstyring hos modtageren

Som det fremgår af figur 2 udføres den omvendte proces hos modtageren. Code Word

7.1.3 Åbne og lukkede systemer

For at begrænse muligheden for hacking har man valgt ikke at standardisere CA systemet. Det at der ikke findes åbne standarder har den ulempe at brugerne kan blive fanget i inkompatible lukkede systemer. Dette kan i værste tilfælde resultere i store omkostninger hos brugerne hver gang de skal skifte serviceudbydere eller komplementere deres services fra forskellige udbydere. Ulemperne ved lukkede systemer og DVB organisationens forslag om en slags interoperabilitet er blevet diskuteret i DVB rapporten[9]. Følgende er baseret på uddrag fra DVB rapporten.

Umiddelbart kan der tænkes to situationer:

Adgangsstyringen bliver standardiseret således, at alle betalings-tv-operatører bruger samme system. Fordelen ved denne løsning er, at en betalings-tv-operatører kan nå alle brugerne. Ulempen, som i praksis gør løsningen mindre attraktiv, er, at når systemets adgangsstyring en gang er brudt / hack'et, ligger det åbent, indtil systemet er ændret.

- Der bliver anvendt proprietære systemer. Denne løsning er ikke mere immun overfor hacking, men det er i givet fald kun et enkelt system, der berøres. Løsningen har den klare ulempe, at brugerne kun kan få adgang til de programmer, der formidles via netop dette system.

For at begrænse ulemperne for brugerne i forbindelse med betalings-tv-operatørernes anvendelse af forskellige adgangsstyringssystemer har DVB-projektet fastlagt to løsningsmodeller, som muliggør, at en bruger kan modtage krypterede programmer med én og samme dekoder, uanset at der benyttes forskellige adgangsstyringssystemer i forbindelse med udsendelsen af de pågældende programmer:

Simulcrypt-løsningen er baseret på, at operatørerne indbyrdes aftaler at varetage adgangs-styringen for hinanden, så f.eks. en del af operatør A's programmer bliver tilgængelig for operatør B's dekodere og

vice versa. Det sker i praksis ved, at der træffes aftale mellem A og B om, at de hver især både sender adgangsstyringsinformationer til egne dekodere og til samarbejdspartnerens dekodere. For at undgå at A og B får kendskab til identiteten af hinandens koder, kan udvekslingen af adgangsstyringsinformationer ske elektronisk og i krypteret form. Set fra brugerens side vil der blot skulle etableres ét kundeforhold med enten operatør A eller med operatør B, og anskaffes den tilhørende dekoder.

Multicrypt-løsningen (Common Interface) er baseret på, at brugeren anskaffer en dekoder, hvor adgangsstyringen varetages af ét eller flere indstiksmoduler efter PCMCIA-standarden. Der anskaffes et modul for hvert adgangsstyringssystem, som brugeren ønsker at være tilknyttet, dvs. normalt et modul pr. betalings-tv-operatør. Dekoderen kan bestykkes med flere moduler samtidig, og brugeren vil kun bemærke, at der er tale om forskellige operatører i forbindelse med fornyelse af abonnement o.lign. Multicrypt løsningen indebærer den fordel, at der ikke er behov for samarbejde mellem konkurrerende operatører, lige som omkostningerne til udskiftning af adgangsstyringssystem - f.eks. hvis kodningen bliver brudt - begrænser sig til omkostningerne ved udskiftning af indstiksmodulet.

7.1.4 Forskellige adgangsstyringssystemer i Europa

Følgende tabel (tabel 1) viser de forskellige CA systemer, som er i funktion i forskellige Europæiske lande.

Systems	Designer
Viaccess	France Télécom
Mediaguard	Seca
Beta-Research	Irdeto
Nagravision	Kudelski
Videoguard	News Data System
Digicipher II	General Instrument
Conax	Conax Telenor

Tabel 1 *CA systemer i Europa*

I Danmark anvender Canal Digital, som den eneste digitale satellit-tv-operatør Conax system og Tele Danmark anvender Viaccess i Tele Danmarks digitale kabel-tv udbud. Canal Digital anvender også Conax systemet i andre nordiske lande og Telia anvender tillige med Tele Danmark Viaccess systemet i deres digitale kabel-tv-udbud.

Tabel 2 viser en detaljeret oversigt over hvilke systemer, der er anvendt i hvilke Europæiske lande:

Land	**Service**	**CA System**
Frankrig	Canal Satellite (Sat)	Mediaguard
	Numéricable (Kabel)	Mediaguard
	Absat (Sat)	Viaccess
	TPS (Sat)	Viaccess
	Lyonnaise Câble (Kabel)	Viaccess
	FTC (Kabel)	Viaccess
UK	Sky Digital (Sat)	Videoguard
	On Digital (Jordbaseret)	Mediaguard
Tyskland	DF1	Beta Research

	Première Digital (Sat)	Beta Research
	T-Medianet (D.T.) (Kabel)	Beta Research
Italien	Stream (Sat)	Beta Research
	D+ (Sat)	Beta Research
Spanien	Via Digital (Sat)	Nagravision
	Canal Satelite (Sat)	Mediaguard
Nordiske lande	Canal Digital (Sat)	Conax
	Senda (Jordbaseret)	Viaccess
	TeleDanmark (Kabel)	Viaccess

Tabel 2 *CA systemer i Europa, mere detaljeret*

En vigtig ting som i denne forbindelse er værd at bemærke, er at nogle af disse systemer f.eks. Viaccess har været operationelle i andre Europæiske lande f.eks. Frankrig og der har ikke været tegn på at systemet er blevet brudt endnu. Dette forstærker argumentationen for at de digitale CA systemer er mere robuste end de analoge.

7.1.5 Administrative sikkerhedsmæssige tiltag for at begrænse pirateri

Fra standardiseringsorganerne har man etableret sikkerhedsmæssige procedurer, hvor de dele af standarderne, som kan være mål for pirateri bliver udleveret til relevante producenter under strenge "Non-Disclosed" aftaler[10].

7.2 NORDIG

NorDig er et strategisk samarbejde mellem tv-selskaber og televirksomheder for indførelse af digital tv i Norden. I NorDig samarbejdet udvikles der bl.a. standarder for en digital dekoder (Set-Top-Box) kaldt NorDig boksen. Det er planlagt at kravene til NorDig boksen bliver udarbejdet i 2 faser. Fase 1 som er gyldig fra slutningen af 1998 (NorDig I) og fase 2 som er gyldig fra slutningen af 1999 (NorDig II). NorDig I specifikationerne, som primært drejer sig om hardware platformen af boksen er færdige og Nordig II specifikationerne, som specificerer softwaren i boksen bliver færdig i 1999.

M.h.t. adgangsstyringen har man i NorDig valgt at basere sig på den åbne "Common Interface" standard. Forskellige CA systemer kan altså anvendes i NorDig boksen blot man erhverver sig en PCMCIA modul, som håndterer det pågældende CA system

NorDig gruppen representerede per første august 1998 følgende broadcastere, operatører og serviceudbydere i de nordiske lande:

Danmarks Radio (DR), Tele Danmark, TV2/Danmark, Helsinki Media, MTV3, Sonera, Yleisradio (YLE), Rikisutvarpid (RUV), Landsimi Island, Canal Digital, Norsk Rikskringkasting (NRK), Telenor, TV2 Norge, Canal+, Modern Times Group (MTG), Scandinavian Broadcasting Service (SBS), Senda, Sveriges Television (SVT), TV4 Sweden, Telia, Teracom

7.3 PIRATKOPI-PROBLEMET I TV'S DIGITALE TIDSALDER

I dette afsnit beskrives de dele af adgangsstyringsystemet, som er beskrevet ovenfor for mulighed for hacking.

Et af kernemodulerne er scrambleren og scrambleren kan hackes. Dette kan ske enten ved at man optager flere talsekvenser (tal1 ..tal n) og regner baglæns til hvilken algoritme, der har generet disse talsekvenser eller også ved at denne information lækker ud af de manufakturer som f.eks. designer Set-Top-Boxe og som på lovlig vis har fået fat i algoritmen.

Et andet af modulerne er Kode Ord (CW) generator. Hvis man vælger en rigtig tilfældig-tal-generator kan dette aldrig hackes. Som pirat vil man her vælge at trække kodeordet ud fra den indkommende strøm og afkryptere det. Dette vil dog være et vanskeligt job, fordi informations lækage fra CA system udbydere er meget lidt sandsynligt og fordi de kan ændre krypteringsalgoritmen hele tiden. At prøve sig frem med forskellige kodeord for at ramme det rigtige vil også praktisk talt være umuligt, da kodeordene ændres så hyppigt.

Selv hvis man har held med at bryde disse dele af systemet skal der stor indgriben i hardware og softwaren på Set-Top-Boxen for at erstatte disse med pirat moduler. Dette er dog lidt nemmere når det drejer sig om pc-kort, idet man her kan bruge pc'ens regnekraft til hjælp, men stadigvæk er det ikke trivielt.

En anden mulighed, som vil være nemmere set fra brugernes synspunkt (altså de brugere der vil snyde), er hvis piraterne kan kopiere smart kortene og evt. modificere dem således at systemet ikke kan detektere, om de er falske.

7.4 KONKLUSION
Adgangsstyringssystemer (CA-systemer) i digital tv transmission er mere robuste mod "hacking" i forhold til de analoge systemer. De teknologier, som er til digitale CA systemer gør det meget svært at være hacker i den digitale tidsalder. Der kræves mere viden, udstyr, regnekraft mm. for at bryde digitale CA systemer. Alene det faktum at der ikke er nogen indikation for hackning af disse systemer i andre europæiske lande hvor digitalt tv har eksisteret i længere tid forstærker gyldigheden af ovenstående påstand[11].

Overgangen til digital TV vil ikke komme piratkiggeri til livs, men dette bliver dog meget mere begrænset. Selvfølgelig kan det ikke foventes, at et digitalt system vil være 100 procent sikkert.

8. Muligheder for lovgivning.

I det følgende afdækkes det handlerum, der er til rådighed i forbindelse med mulighederne for gennem lovgivning at forhindre tv-pirateri.

Med udgangspunkt i de forekommende former for tv-pirateri beskrives de områder, der kan sættes ind overfor og senere beskrives de evt. konsekvenser.

Der er foretaget en opdeling af casen på aktører, varer/services, handlinger og distributionskanaler. Blandt disse kategorier kan de lovgivningsmæssige handlemuligheder identificeres. Det kan vurderes i hvilke søjler og rækker i matricen, der er mulighed for en hensigtsmæssig lovændring.

Som udgangspunkt kan beskrives to ulovlige former og en lovlig form for uautoriseret adgang til betalings-tv-kanalernes udsendelser: (piratkiggeri)

I den første form for piratkiggeri, der på nuværende tidspunkt er ulovlig, sælges et kort, der i forvejen har fået adressekoden lagt ind. At sælge og købe et sådant kort er ulovligt.

I den anden form for piratkiggeri, der på nuværende tidspunkt er ulovlig, er der tale om kort, der virker fuldstændig som de autoriserede kort - og som altså opdateres automatisk. Disse kort har som tidligere nævnt en ringe udbredelse.

Blandt de tre grundformer for piratkiggeri vil udelukkende den herunder illustrerede lovlige form blive analyseret yderligere.

8.1 VÆRDIKÆDENS KOMPONENTER
Herunder beskrives handlemuligheder for de enkelte komponenter i værdikæden.

8.1.1 Paraboler og tunere/set top bokse
Med udgangspunkt i de enkelte varer eller serviceydelser, der muliggør pirateri, betragtes nu parabolen og den tilhørende receiver/set-top-box. Det er umiddelbart indlysende, at et forbud mod salg af paraboler er perspektivløst. Forhandlerens handling (salg) er uundværligt hvis det overhovedet skal være muligt at se satellit-tv. At forbyde tv- og radioforretninger er lige så utænkeligt – og det samme gælder for lovgivning, der sigter mod genstandene selv: et forbud mod import eller produktion af udstyret er heller ikke realistisk. Ligeledes er det ikke hensigtsmæssigt at forbyde privatpersoner at eje paraboler og dekodere/set top bokse.

I de øvrige dele af værdikæden er der større mulighed for gennem lovgivning at imødegå pirateri.

8.1.2 SmartCards og brændere
Forhandlere af SmartCards udbyder en vare, der finder anvendelse i adskillige legale sammenhænge, så hverken salget eller varen i sig selv kan gøres til genstand for forbud uden omkostninger i andre sammenhænge. Et forbud rettet specifikt mod salg til en defineret gruppe (eksempelvis private i modsætning til virksomheder) er en mulighed, men dels vil det næppe forhindre en energisk pirat, dels vil det lægge hindringer i vejen for anden privat anvendelse.

8.1.3 Software
Den software, der lægges på kortet er ofte programmeret til lovlige formål og som i forbindelse med kort og brændere, er der tilsvarende omkostninger forbundet med at indskrænke distributionen af software'n. Dertil kommer, at distribution ad internettet er vanskelig at forhindre og - såfremt software'n distribueres i krypteret form - endnu vanskeligere at bevise.

8.1.4 Operationskode
Hacker'rens aktivitet (at finde operationskoder med udgangspunkt i kendte management keys og de fra satelliterne udsendte signaler [check med DW om det er sådan, det foregår] har udelukkende til formål at sætte ikke-abonnenter i stand til at se de krypterede signaler. Et forbud mod denne aktivitet rammer derfor ikke andre sektorer. Et forbud mod distribution af operationskoderne er ligeledes uden utilsigtede konsekvenser, men da koderne ofte distribueres ad internettet eller SMS, må det forventes vanskeligt at påvise og bevise distribution. For den til kortet hørende software såvel som operationskoder gælder, at en indskrænkning i den almindelige anvendelse af distributionskanalerne (internet og SMS) ville lægge væsentlige begrænsninger på kommunikation i almindelighed.

8.1.5 Privatpersoners piratkiggeri
Tilbage er nu sidste led i værdikæden: pirat-seeren. Et forbud mod privat besiddelse af SmartCards, brændere og software vil som tidligere anført forhindre andre (legitime) anvendelser. Et forbud mod erhvervelse og anvendelse af operationskoder må forventes vanskeligt at håndhæve - igen fordi det er vanskeligt at på- såvel som at bevise. Tilbage er så et forbud mod piratkiggeriet selv: anvendelsen af de i værdikæden beskrevne genstande og oplysninger. Det er her, Canal Digital og ViaSat ønsker, at der sættes ind med en lovændring. Her må det overvejes, om den (positive) signalværdi der ligger i at forbyde utilsigtet tv-kiggeri opvejes af den (negative) signalværdi, der ligger i et forbud, der vanskeligt

kan håndhæves. Dertil bør det overvejes, hvordan en sådan lov kan administreres i praksis.

8.2 ER DEN UDBREDTE FORM FOR PIRATERI KRIMINEL ?
Vurderet i forhold til den nuværende lovgivning i Danmark er der intet ulovligt i det ovenfor skitserede forløb. Imidlertid vil visse former for offentliggørelse af operationskoder falde under begrebet "erhvervsmæssig anvendelse". Dette er tilfældet, hvor koderne bruges til at tiltrække sig opmærksomhed omkring andre produkter eller services, der bringes i omsætning i sammenhæng med operationskoderne.

Mange af pirat-siderne har formentlig indtægter i form af banner-reklamer, adultcheck (adgangsbetaling) til porno m.v. Der er således mulighed for at retsforfølge en væsentlig del af de personer, der offentliggør koder. Der er dog risiko for, at de i givet fald flytter deres sites til en udenlandsk server, hvor retsforfølgning og efterforskning er vanskelig.

Med henblik på muligheden for at forhindre pirateri ved at retsforfølge de, der bruger koder som "lokkemad" til andre varer eller services, er der foretaget en tentativ undersøgelse af udbredelsen af reklamering for eller salg af andre varer eller tjenesteydelser i forbindelse med satellitkoder. De undersøgte websites og omfanget af deres reklamer m.v. ses af tabellen i bilag 3.

Konklusionen på den oversigtsmæssige undersøgelse er, at der stadig er så mange idealistiske/ej reklamedrevne offentliggørere, at man ikke kommer problemet til livs ved at slå ned på porno-sites'ene.

9. Forventede konsekvenser af forskellige lovændringer

9.1 INDLEDNING
Dette afsnit har til formål at vurdere effekten af forskellige stramninger af lovgivningen angående uautoriseret dekodning af radio- og tv-signaler, særligt med det formål at se på effekten af et forbud mod benyttelsen af uautoriserede kort.

9.2 GENERELLE OVERVEJELSER
Generelt må der foretages en afvejning af ønsket om at forbyde uønskede forhold med de begrænsede muligheder for håndhævelse af forskellige overtrædelser og karakteren af de potentielt uønskede forhold.

I denne forbindelse er det væsentligt, at en reel kontrol af hvorvidt piratdekoderkort forefin-des i private hjem kun vil kunne gennemføres ved hjælp af en omfattende ransagning af det private hjem. En sådan ransagning kan, set i forbindelse med forbrydelses størrelse, næppe anses for at være i overensstemmelse med proportionalitetsprincippet.

Det må derfor forventes at privatbrug af piratdekoder kort kun opdages i forbindelse med efterforskningen af andre former for kriminalitet.

Endvidere må det anføres, at betalings-tv-selskaberne har kendt til den lovgivning, der fandtes på området da de valgte at gå ind på markedet.

9.3 PARALLELLER TIL ANDRE BRANCHER
Fremstillingen og brugen af piratdekoderkort kan til en vis grad sammenlignes med fremstillingen og brugen af piratsoftware. Der er dog den væsentlige forskel, at salget i softwarebranchen foregår til både virksomheder og private, mens betalings-tv-branchen stort set udelukkende har private kunder.

I softwarebranchen er udbredelsen af piratsoftware dog ikke ligeligt fordelt mellem private og erhvervskunder. Således antages det generelt, at andelen af pirateret software hos private er langt større end andelen hos virksomheder.

På udbudssiden har software branchen gennem forskellige brancheorganisationer valgt at bekæmpe udbredelsen uanset om kunden er privat eller en virksomhed, men på efterspørgselssiden har branchen valgt hovedsageligt at gå efter virksomheder, mens privat brug at piratsoftware er forholdsvis sjælden.

Selv om både fremstilling og brug af piratsoftware er forbudt er de facto forholdene på markedet således, at en vis grad at piratsoftware i private hjem om ikke accepteres, så tolereres. Da både fremstilling, salg og brug af piratsoftware er forbudt er forholdene på dette område således, at en kriminaliseret aktivitet i realiteten tolereres i en meget stor del af de danske hjem.

9.4 KRIMINALISERING AF PRIVAT BRUG AF PIRATDEKODERKORT

Det må anses for sandsynligt, at en stramning af loven, der gør privat brug af piratdekoder kort ulovlig hovedsagelig vil have en signalvirkning. En reel og konsekvent håndhævelse af forbudet er næppe mulig. En signalvirkning fra en stramning af loven må dog anses at have en noget større værdi hvis der, som det er sket i Norge gennemføres aktioner, der signalerer til borgere at brug af piratdekoderkort ikke alene er forbudt, men også er forbundet med konsekvenser.

Selv om det må anses for sandsynligt, at en del borgere, der i dag benytter piratdekoderkort vil rette sig efter et eventuelt forbud, må effekten af et sådant forbud anses for begrænset. Ikke mindst fordi det er vores opfattelse, at en relativt stor del af befolkningen mener, at privat brug af piratdekoderkort er ulovlig eller i hvert fald umoralsk.

Modgående disse argumenter må norske erfaringer dog anføres. Her angiver betalingsselskaberne at deres penetrationsgrad er langt højere mens antallet af pirater i Norge er væsentligt mindre end i Danmark og Sverige. Samtidig er det væsentligt sværere at finde norske sælgere af piratkort og -koder på Internettet. Der findes dog ikke en undersøgelse på linie med den i Danmark foretagne Vilstrup-undersøgelse[12] der kan be- eller afkræfte disse forhold. Da den norske lovgivning forbyder brugen af uautoriserede dekoderkort kunne dette tyde på, at et sådant forbud har en effekt.

9.5 BRÆNDERE OG BLANKE KORT

Et forbud mod salg af brændere og blanke kort må anses for at være uhensigtsmæssigt. De blanke kort anvendes til forskellige andre formål, herunder sikringssystemer. Komponenterne til brænderne er helt generelle elektronik-komponenter, som anvendes til mange formål, og det er næppe realistisk at forbyde dem. Det er tilsyneladende ikke almindeligt, at komponenterne sælges færdigsamlet i detailhandlen, men nok i et samlesæt med brugsanvisning til samling. Et forbud mod dette vil besværliggøre pirateri, men formodentlig ramme ganske få, idet det må antages, at pirater vil importere den nødvendige hardware fra udlandet - f.eks. som elektronisk handel på Internettet og ligeledes hente brugsanvisninger her.

9.6 FORBUD MOD OFFENTLIGGØRELSE AF KODER PÅ INTERNET ELLER LIGN.

Et vigtigt element i den uautoriserede adgang til betalings-tvkanalerne er en nem og hurtig adgang til de nødvendige opdateringskoder til piratkortene. Internettet spiller en væsentlig rolle i offentliggørelsen af disse koder. Et effektivt forbud mod en sådanne offentliggørelse må dog anses for urealistisk. Dels kan piraterne vælge at placere deres hjemmesider på servere udenfor Danmark og dermed omgå dansk lovgivning. Dels kan piraterne vælge at gemme koderne bag en adgangsbegrænsning. En sådan vil vanskeliggøre en efterforskning af, om opdateringskoder videregives betydeligt, men vil nok også

begrænse eller forsinke spredsningshastigheden for koderne.

Endeligt spredes koderne også, i et ikke ubetydeligt omfang via f.eks. e-mail eller SMS beskeder sendt til mobiltelefoner. Et stop for sådanne mailinglister må ligeledes anses for stort set umuligt.

10. Konklusion

I EU-direktivet om retlig beskyttelse af adgangsstyrede og -styrende tjenester fra d. 28. november 1998 har man ikke fundet det hensigtsmæssigt at påbyde strammere regler end de nuværende danske. Der åbnes dog mulighed for at de enkelte stater indfører en strammere regulering.

Ønsket om en stramning af lovgivningen vedr. piratdekoderkort mv. kommer helt overvejende fra betalings-tv-stationerne og er begrundet med det angiveligt store omfang af piratkiggeri. Det fremgår af analyserne ovenfor, at der næppe er tvivl om, at piratkiggeriet har et betragteligt omfang. Ud fra hensyn til krænkede oprethavsrettigheder mm. kunne det umiddelbart synes at begrunde en stramning af lovgivningen på området. Der er dog en række forhold, der må overvejes i denne forbindelse:

Det er næppe tænkeligt, at en kriminalisering af privat besiddelse vil blive efterforsket seriøst.

Kriminalisering af aktiviteter, som man ikke kan eller vil efterforske seriøst, kan være betænkelig ud fra hensyn til afsmittende virkning på retsopfattelsen.

Kommerciel overdragelse er allerede på nuværende tidspunkt forbudt. Et forbud mod anvendelse af kortet vil kun ramme de få piratseere der har fulgt den tidligere beskrevne lovlige fremgangsmåde til uautoriseret adgang (jvnf. afsnit 8).

En lov rettet mod selve anvendelsen af piratkort vil således være et supplement til den eksisterende lovgivning, der i sig selv kun rammer få.

Et forbud mod salg af brændere og blanke kort er næppe hensigtsmæssigt, idet blanke kort og komponenterne i brændere anvendes andre formål.

Branchen har selv gode handlemuligheder, idet digital tv transmission er meget robust overfor hacking – en overgang til digital TV vil næppe komme piratkiggeri til livs, men må antages at begrænse det betragteligt.

Hacking af koder mm. er stadig præget af entusiaster/ amatører, men der kan konstateres en kommercialisering af værdikæden, der fører frem til brugernes besiddelse af piratkort.

Umiddelbart synes ovenstående at føre til en konklusion om, at lovgivningen i forbindelse med overdragelsessituationen ikke burde strammes op. Der findes dog allerede lovgivning, ifølge hvilken mindst ét led i værkdikæden er ulovligt for langt størstedelen af piratkiggeriet. Det må desuden erindres, at Udvalget vedrørende Datakriminalitet såvidt vides arbejder med forslag, der ligestiller spredning af data med erhvervsmæssigt brug.

Bilag 1: Erfaringer på Center for Tele-Information med fremstilling af piratkort

At fremstille sine egne pirat-dekoderkort er ikke nogen let sag. CTIs medarbejdere forsøgte under udarbejdelsen af denne rapport at fremstille pirat-dekoderkort. I forløbet viste der sig en del

vanskeligheder, der må forventes at afskrække den almindelige potentielle tv-pirat fra selv at forsøge sig.

Ved fremstilling af egne pirat-dekoderkort er følgende nødvendigt:

- En smartcard-brænder
- En computer
- Et blankt kort (et smartcard)
- Et stykke brændersoftware til computeren
- Software til kortet

Ideen er så, at brænderen forbindes til computerens COM-port, brændersoftwaren indlæses, det blanke kort indsættes i brænderen, og software'n til kortet føres over på dette. Der er imidlertid ved stort set alle led i denne proces risiko for betragtelige problemer. Disse potentielle eller reelle problemer præsenteres herunder - opdelt på hvert enkelt af processens led.

BRÆNDER
Det var ikke muligt at købe en færdigmonteret brænder. En henvendelse i en af Københavnsområdets største elektronikforretninger (Brinck Elektronik) resulterede kun i køb af et samlesæt, idet butikken ikke ville sælge færdige brændere af frygt for at komme i konflikt med lovgivningen. Et sådant samlesæt består af en printplade samt en ganske betragtelig mængde elektroniske komponenter, der skal påloddes pladen. En brugsanvisning medfulgte, men for en person, der ikke er øvet i lodning af elektronik, er det aldeles umuligt at montere brænderen.

Herover ses brænderens forskellige komponenter .Som eksempel på vanskeligheden ved montering tjener desuden følgende uddrag af brugsanvisningen:
"Det er vigtigt at sikre sig, at alle ben er kommet igennem printpladen inden der loddes. Husk at varme på både ben og print-ø med en let fortinnet varm loddekolbespids og tilføj dernæst rigtig elektronikloddetin mellem ø og ben. En god (blank) lodning tager max 10 sek. Dernæst monteres alle modstande. Husk at bukke benene let ud til side og afklippe disse 1-2 mm over kobberbanerne inden der loddes. Af trådafklippende laves, isættes og loddes nu de 5 lus, der er vist som streger. Dernæst monteres vendt rigtigt dioder, transistorer og elektrolytter."

Der er tydeligvis meget, der kan gå galt for en utrænet hobby-lodder. Det kan ikke udelukkes, at der er butikker, der sælger færdigmonterede brændere, men disse kan formentlig ikke findes uden et godt kendskab til branchen. Prisen på brænderen må desuden forventes at være væsentligt højere end de 155 kr, samlesættet koster.

COMPUTER
En computer (med internet-opkobling, som er en forudsætning for fremskaffelse af den nødvendige software)findes i mange hjem, og denne forudsætning er derfor for en del potentielle piraters vedkommende opfyldt. Et problem i denne forbindelse er, at der under brændingsprocessen er risiko for at overbelaste computerens COM-port. En ny com-port med tilhørende controller koster omkring kr. 200,- til 300,-. Den økonomiske risiko i denne forbindelse er ganske vist til at overskue, men udsigten til at skulle montere ny port og controller i hjemme PC'en vil nok afskrække en del.
Blanke kort

Som råmedier til piratkortene bruges blanke smartcards. De er i sig selv ukomplicerede, men brændingsprocessen er behæftet med en vis risiko for fejlbrænding, hvorved det rå kort ødelægges. Med en pris på kr 100,- pr smartcard skal der ikke brændes meget forkert, før det bedre kan betale sig at

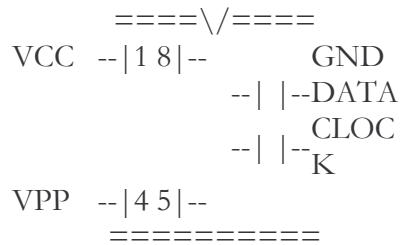
abonnere på en betalings-tv-kanal.

BRÆNDERSOFTWARE
At fremskaffe og installere den nødvendige brændersoftware er heller ikke helt ligetil. Igen kan et uddrag af monteringsvejledningen tjene til illustration:
"De nødvendige programmer og filer, for at kunne brnytte Br875 må man selv hente og finde på internet.... Et meget benyttet og udmærket program er PIP02 vers. 1.18 (PIP02 vers. 1,26 er noget fejlbehæftet og bør derfor ikke anvendes - versioner for 1.18 giver også problemer med PIC12C508). For at kunne benytte PIP02 må man først indlæse driveren BR875.EXE."

Et sådant program kan lokaliseres og downloades fra internettet, men igen mødes en eventuel bruger af et uforståeligt sprogbrug. De eneste brugsanvisninger, der fandtes i forbindelse med programmet var af følgende type:

PIC12C508 FEATURES
Program memory (OTP/EPROM): 1024 bytes
Program memory word size: 12 bits
Package: DIP-8, SO-8

Connection Diagram for programming
(Both DIP8 and SO-8 Packages



...hvilket må siges at være komplet uforståeligt for en lægmand.

SOFTWARE TIL KORTET
Ud over den software, der styrer selve brændingsprocessen, er det også nødvendigt at finde og downloade den software, der skal føres over på smardcard'et. Dette er ikke i sig selv vanskeligt, idet en del af de websider, der videregiver operationskoder, også har links til den nødvendige software.

Problemet opstår først, når software'n er downloaded. Et eksempel er Multimac-filen (fundet på http://www.pyro.dk/). Her er den eneste medfølgende vejledning følgende

Disse hex-filer kan bruges til Galaxykort, Goldkort & Platinkort.
Mm2_rb7.hex er til 16X84 chippen.
Mm2_eep.hex er til 24C16 chippen.

Disse oplysninger er vanskelige at anvende - især da der ikke på smartcard'et står noget om hvilken slags chip, der er monteret på det.

KONKLUSION
Af ovenstående gennemgang fremstår det klart, at brænding af egne dekoderkort ikke er nogen overskuelig opgave for den almindelige tv-seer. Det må forventes, at langt størstedelen af de, der ønsker at se satellit-tv med et piratkort vil undgå denne fremgamgsmåde til fordel for køb af et (ulovligt) forprogrammeret piratkort. Selv om enkelte trin i processen lettes - eksempelvis ved, at det lykkes at købe en færdigmonteret brænder - resterer der stadig rigelige hindringer for et heldigt udfald af den lovlige fremgangsmåde til fremstilling af piratdekoderkort.

Bilag 2: Undersøgelse af holdninger og bevæggrunde i piratmiljøet

Med henblik på belysning af piraternes synspunkter og position har CTI udsendt en email til folkene bag 11 af de mest benyttede websites, der bringer D2Mac-koder. Hensigten var at tilvejebringe information fra andre kilder end udbydersiden. Spørgsmålene fokuserede på, piraternes bevæggrunde, den faktiske udbredelse af piratkiggeri samt de eventuelle effekter af lovændringer og digitalisering.

De 11 modtagere blev valgt blandt de websites, der figurerede på D2Mac listens top 25. Kriteriet for udvælgelse var dels, at der var en dansker bag websiten, dels at der var mulighed for at kontakte den pågældende person - og her var email stort set den eneste mulighed.

Fra D2Mac listen på http://twm.dk/topsites/topsites.html

Titel	URL	Bannere	Salg af kort og andet udstyr	Bemærkninger
Den Skandinaviske Satellit Side	http://www.dsss.dk/	Ingen	intet	
NIELSEN'S D2MAC	http://home6.inet.tele.dk/musen/	PL telefoni (formentlig eget selskab) - ellers ingen	intet	
Pyro`s Kodeservice	http://www.pyro.dk/	Egen PC-butik, "loppemarked"	intet	
Mr.Satellite's Homepage	http://hjem.get2net.dk/mr_satellite/	ingen	linker til kortsælgere, men ingen åbenbar sammenhæng	
D2mac World	http://home10.inet.tele.dk/frn/	porno-websites	link til sælger af waferkort og brændere	
Cheaters Heaven - @ - www.cheaters.dk	http://www.cheaters.dk/	Link Exchange, Bannerswap	Ingen	
Don's Satpage	http://home2.inet.tele.dk/brinch/	Banner for Eldanmark (Parabolfirma)	Ingen	
SATWARE.DK	http://www.satware.dk/	ingen	intet	
TSK Sat Site	http://hjem.get2net.dk/tsk/side.htm	Ingen	Intet	

Sejersen´s Homepage	http://home8.inet.tele.dk/sejersen/	ingen	intet	Familiehomepage med link til koder
D2MAC-DK	http://members.xoom.com/D2MacDK/	ingen	intet	

MODTAGERE AF EMAIL-HENVENDELSE

Responsen på henvendelsen var sparsom: To af de adspurgte returnerede emailen med - den ene med meget kortfattede svar (s1), den anden med noget mere uddybende kommentarer (s2). En tredje lagde henvendelsen ud på sin website med sin egen kommentar tilknyttet. Bortset herfra var der ingen synlig reaktion.

Med henblik på at identificere eventuelle reaktioner i pirat-miljøet, blev nyhedsgruppen dk.medier.satellit observeret i dagene efter henvendelsen. Her var ingen omtale af henvendelsen at spore.

På basis af den ringe respons kan der ikke umiddelbart konkluderes noget. Den modtagne svar-email indeholdt kun uunderbyggede påstande. Det eneste område, hvor der er skabt mere klarhed er omkring piratkodedistributørernes bevæggrunde. Her svaredes, at formålet med at offentliggøre de fundne koder på en website er, at man derved undgår telefoniske henvendelser fra folk, der ønsker koden oplyst - og som formentlig på forhånd kendte til, at den pågældende var i besiddelse af koderne. En lignende anskuelse er blevet fremlagt i dk.medier.satellit, hvor det Rene Beining den 18. december 1998 skriver:

" Både udbydere og hackere har lært af det her "D2-MAC cirkus" hvor enhver "amatør" har de sidste nye koder på deres homepage. Det skal ikke forstås at jeg er bedre end andre, jeg havde også en homepage i midten af 95. Problemet er bare at det blev for udbredt og begyndte at true udbyderne. Det ødelagde det lidt for os der havde det som hobby."

Begge udsagn tyder på, at i hvert fald de tidlige pirater ikke videregav de fundne koder for personlig vindings skyld.

Dette underbygges også af tabellen, hvoraf det fremgår, at blandt de 11 websites er der ingen, der selv sælger brændere eller smartcards. Der er dog to, der linker til websites, hvor disse varer sælges - og det må betragtes som sidestillet med selv at sælge varerne, da det er en ren teknikalitet, om koder og brændere/kort distribueres via én eller flere websites.

Fem af de elleve havde reklamer på deres websites. Heraf havde én site kun reklamer for LinkExchange og BannerSwap, vilket næppe er indtægtsgivende. Tre havde reklamer for danske firmaer (sandsynligvis personernes egne firmaer), og yderligere én linkede kraftigt til forskellige erotiske websites. Kun sidstnævnte kunne formodes at være direkte indtægtsgivende.

Der er således ikke umiddelbart belæg for at påstå, at personerne bag de undersøgte websites i almindelighed videregiver koderne for egen vindings skyld.

FORSKELLIGE FORMER FOR RESPONS PÅ DEN UDSENDTE MAIL:

Herunder er de stillede spørgsmål samt svarene fra de to respondenter angivet:

Hvor mange piratkiggere til Canal Digital og ViaSat findes der i Danmark?

s1: Det skal stilles i forhold til hvor mange parabolejere der findes. Ca. 90 % anvender pirat -kort
s2: Et rimeligt skøn er at der er ca. 100.000 - 130.000 "piratkiggere" i Kongeriget Danmark, og ikke én disse mer' ..

Tror du på Canal Digitals og ViaSats påstand om, at der er 250.000 piratkiggere i Danmark?
s1: se ovennævnte
s2: Så absolut ikke.. De prøver for det meste kun at overdramatisere de forskellige tal, og dermed forsøge at gøre "problemet" til at lyde meget større end det i virkeligheden ér!

Hvor mange piratkiggere ville blive legitime abonnenter, hvis piratkiggeri blev gjort ulovligt ?
s1: 1-2 %
s2: Efter min mening, og kendskab til folk, så vil jeg ikke mene at der er mere en 5-10% der vil begynde at betale, hvis det skulle gå hen og blive ulovligt.

Ville en større risiko for opdagelse begrænse den allerede på nuværende tidspunkt ulovlige distribution af piratkort ?
s1: Nej
s2: Der er efter min mening absolut ingen grund til at tro at der er en storstilet organiseret distribuering af ulovlige piratkort i Danmark... Igen en af de mange af CD* og VS** skrøner!! - Om der er nogen grund til at skærpe kontrollen/undersøgelserne om der er folk der gør sådanne ting, mener jeg er fuldstændig et skud i luften, da hvis der er nogle enkelte personer der distribuerer kort, så er de klar over konsekvenserne for deres handlinger, hvilke efter min mening er rimeligt høje i forvejen (straffen for ulovlig distribuering - 75§)...

Hvad driver piraterne ? Økonomisk vinding eller lyst til at demonstrere sin dygtighed (eller noget helt andet) ?
s1: Så er man fri for at folk ringer og spørger efter koderne.
s2: 5. Hvad der driver os? Tjaa, vi har det som en hobby, og har ingen kommercielle hensigter.. At der måske er få personer der udnytter de muligheder der byder sig, er måske rimeligt nok, for der ligger også en del arbejde bag.. At det resulterer i tab for selskaber som CD* og VS** er en af bagdelene, men det kan ikke undgås, og skulle det blive ulovligt, så vil jeg bi-beholde min holdning, og fortsætte mit arbejde.

Er der økonomisk gevinst for indehaverne af satellit-hjemmesider ved at videregive operationskoder (eksempelvis forøgede indtægter gennem bannerreklamer) ?
s1: Nej
s2: He He..Den var god.. I og med at jeg selv har en satellit-side, ved jeg af egen erfaring, at der kun følger udgifter med en sådan side... At der er nogen der bestemmer sig for at knalde et par reklamer på deres sider, syntes jeg er helt iorden... Jeg kan ihvertfald sige at jeg har en gennemsnitlig udgift på ca.4000-5000kr hvert kvartal som jeg skal betale til teleselskabet.. Dem tjener jeg så ved arbejde, og ikke ved at sælge piratkort...!!!

Er de tal, hjemmesidernes hit-countere viser, korrekte (eller er der "justeret" på dem for at give indtryk af større trafik) ?
s1: De er korrekte
s2: Om counterne viser rigtigt.. Jaa, gu gør de da det.. hvorfor skulle vi stille på dem? Jeg har et gennemsnit på 2000-4000hits pr. døgn hvilket er meget alm. for en større satellit-side.. Det er jo ikke kun koder vi udgiver, men også alm. information inden for TV og satellit verdenen...

Vil fremtidig digital udsendelse af signalet gøre det svært for piraterne at operere ?
s1: Næppe
s2: Tjaa, een ting er helt sikker, hvilket er at: Ligemeget hvad de bestemmer sig for, så er der folk der er villige til at knække/hacke deres systemer, og for ikke engang at sige noget helt hen i skoven, så ér alle nye systemer knækket/hacked indenfor få måneder !!!

Respondent 2 tilføjer desuden:

En konklusion på hele besvarelsen er:
Ligemeget hvad de vil gøre, så vil hjulet ikke stoppe...
Sådan som vi har det nu, syntes jeg ikke at det vil hjælpe at foretage nogen lovændring, da det ikke vil føre til noget, men bare er spild at politikernes og embedsmænds tid..

Reglerne som de er nu, syntes jeg at det fungérer rigtigt godt.. Det er ulovligt at sælge programmerede smartcards i henblik på at afkode betalings-pligtig TV... Det er dermed helt op til forbrugeren selv at beslutte sig for hvad de vil bruge deres tomme smartcard til, og anderledes og bedre kan det ikke blive!!! Man kan jo bruge følgende eksempel som en sammenligning: Hvis en person går hen i en isenkram-butik og køber en køkken-kniv, for så 5min senere hén at slå en forbi-passerende person ihjel med kniven ville Politiet i dette tilfælde ikke tænke så meget som i 5min på at arrestere sælgeren af kniven, da han jo ikke kan gøres ansvarlig for køberens handling..... Det samme princip SKAL også gælde på alle andre områder, og jeg kan derfor ikke se hvorfor det skulle være anderledes med sådanne smartcards?

Én anden ting er for at skrive lidt om satellit siderne:
Det er da imod menneskerettighederne at forbyde folk at skrive en talkombination på 28 numre..!!!
Efter min mening er det helt op til TV-selskabet selv, at beskytte deres Operations-nøgler så godt, at det ikke er muligt for personerne bag satellit-siderne at fremskaffe dem (koderne)...!

CD* = Canal Digital
VS** = ViaSat

---------->

Jeg har ikke nogen form for dokumentation til at underbygge mine svar, så de ting jeg har skrevet ned her i denne mail, er den erfaring jeg har samlet gennem en del år i "branchen"..

Respons 2: Offentliggørelse på hjemmeside af henvendelse
En enkelt blandt de adspurgte besvarede ikke emailen, men offentliggjorde den i stedet på sin hjemmeside.

På åbningssiden kunne følgende tekst læses:
I got an interesting Mail to day,it's about an investigation,that the danish kulture minestery have hired the center for tele communication,to made,unfurtunally it's only in danish,(i dont translate in english)

You can see it here

Hvor ordet "here" var et link til en anden side. På denne fandtes CTIs email ledsaget af følgende kommentar:

HMMM.

Fik denne mail i dag:

Hvis jeg ikke havde tjekket dette ,ville jeg tro det var Jens H.Fra Lars tyndskides mark der havde sendt dette,men det er det sku ikke,de må sku da være lidt for blå øjed,hvis de tror på at nogle vil hjælpe med den undersøgelse,jahhh så tror de sku nok også på spøgelser. ;o)

Ovenstående var at finde på den pågældende website i perioden 23/2 til 25/2 1999.

Respons 3: Diskussion af emailen i nyhedsgrupper
Ingen diskussion af emailen eller undersøgelsen er observeret i nyhedsgruppen dk.medier.satellit.

Den udsendte email:

Kære [website-indehaver]

Center for Tele-Information foretager for tiden en undersøgelse af udbredelsen og formen af pirat-kiggeri i Danmark. Undersøgelsen er et led i et arbejde for Kulturministeriet, der ønsker et beslutningsgrundlag for
et evt. indgreb mod privatpersoners brug af piratkort.

Du får denne email fordi det har vist sig vanskeligt at få forskellige synspunkter i sagen repræsenteret. Canal Digital og ViaSat fremlægger meget gerne deres opfattelse af sagen samt deres overslag over udbredelsen af pirat-kiggeri. Producenter, distributører og brugere af uautoriserede kort og operationskoder er - uanset at deres virksomhed meget vel kan være i overensstemmelse med den nuværende lovgivning - ikke organiseret i samme grad som tv-kanalerne. En interesseorganisation modsvarende Canal Digitals
og ViaSats "STOP" findes så vidt vi ved ikke.

I nedenstående spørgsmål er ordet pirater brugt om alle, der medvirker til at gøre det muligt, at tv-seere uden abonnement kan se kodede tv-kanaler via satellit. Betegnelsen pirater omfatter også de ovennævnte tv-seere selv.

Hvis du er i stand til at underbygge svarene med troværdige kilder, vil vi meget gerne have en henvisning til disse.

Vi håber, du vil tage dig tid til at besvare og kommentere spørgsmålene, hvis du kan - helst inden udgangen af februar. Dine svar vil blive anonymiseret - vi videregiver ikke din identitet - og indgå i vores rapport.

Vi har følgende spørgsmål, som vi meget gerne vil have dine kommentarer til:

Hvor mange piratkiggere til Canal Digital og ViaSat findes der i Danmark ?

Tror du på Canal Digitals og ViaSats påstand om, at der er 250.000 piratkiggere i Danmark?

Hvor mange piratkiggere ville blive legitime abonnenter, hvis piratkiggeri blev gjort ulovligt ?

Ville en større risiko for opdagelse begrænse den allerede på nuværende tidspunkt ulovlige distribution

af piratkort ?

Hvad driver piraterne ? Økonomisk vinding eller lyst til at demonstrere sin dygtighed (eller noget helt andet) ?

Er der økonomisk gevinst for indehaverne af satellit-hjemmesider ved at videregive operationskoder (eksempelvis forøgede indtægter gennem bannerreklamer) ?

Er de tal, hjemmesidernes hit-countere viser, korrekte (eller er der "justeret" på dem for at give indtryk af større trafik) ?

Vil fremtidig digital udsendelse af signalet gøre det svært for piraterne at operere ?

Med venlig hilsen

Alexander Øst
Center for Tele-Information
Bygn. 371
Danmarks Tekniske Universitet
2800 Lyngby
Tlf: 45 25 51 90

Bilag 3: Undersøgte pirat-websites

Fra D2Mac listen på http://twm.dk/topsites/topsites.html

Titel	URL	Bannere	Salg af kort og andet udstyr	Bemærkninger
d2macdecoding	http://www.d2macdecoding.com/main.html	PC Gamer digiweb.dk	Link til http://www.satshop.nu/	
d2dec.com	http://www.d2dec.com/	Ingen	intet	
Den Skandinaviske Satellit Side	http://www.dsss.dk/	Ingen	intet	
WWW.PUT.DK	http://www.put.dk/	Team Internet, InterStat Porno-links Adultcheck	intet	
JJ-sat D2mac	http://welcome.to/jjsat	ingen	Private annoncer	sponsor pag "cards progra "coming soon" medlemskab: 100,- kommercielt perspektiv)
Finders Satellites	http://website.lineone.net/~adr/	mange	Kort sælges (£ 15 - 150) Dekodere og paraboler m.v. sælges	Engelsk websit
NIELSEN'S D2MAC	http://home6.inet.tele.dk/muse	PL telefoni (formentlig	intet	

	n/	eget selskab) - ellers ingen		
JKP´s Daily Updated WaReZ SiTE with D2mac Codes & Mp3 files	http://www.jkp.dk/	ingen	ingen	Diverse hack crack-programm
Pyro`s Kodeservice	http://www.pyro.dk/	Egen PC-butik, "loppemarked"	intet	
"TSS" The Sat Site.	http://home1.inet.tele.dk/fni/	ingen	intet	
Mr.Satellite's Homepage	http://hjem.get2net.dk/mr_satellite/	ingen	linker til kortsælgere, men ingen åbenbar sammenhæng	
D2mac World	http://home10.inet.tele.dk/frn/	porno-websites	link til sælger af waferkort og brændere	
Cheaters Heaven - @ - www.cheaters.dk	http://www.cheaters.dk/	Link Exchange, Bannerswap	Ingen	
Don's Satpage	http://home2.inet.tele.dk/brinch/	Banner for Eldanmark (Parabolfirma)	Ingen	
***** Renè`s Hjemmeside *****	http://members.tripod.com/Lauersen/			virker ikke
SATWARE.DK	http://www.satware.dk/	ingen	intet	
TSK Sat Site	http://hjem.get2net.dk/tsk/side.htm	Ingen	Intet	
Jonas D2macsida	http://www.algonet.se/jonas-n/			Nede
Sejersen´s Homepage	http://home8.inet.tele.dk/sejersen/	ingen	intet	Familiehomepa med link til (hvordan den e top 25 er en gå
Hottest D2-Mac Codes on the net. Mirror for Clanzer's programmer build5.	http://members.tripod.com/~Handy_Man_1/	ingen	intet	
D2MAC-DK	http://members.xoom.com/D2MacDK/	ingen	intet	
Per's D2MAC INFO	http://users.cybercity.dk/~bsq3273/	Playstation-butik	intet	Link til manag key søgefælless
BT's Homepage	http://home9.inet.tele.dk/bruce/	Thor søgemaskine	intet	
Gröna Brigadens Homepage - Tingsryd Fan	http://come.to/brigaden			ingen satellitoplysning
Canal + koderna finns HÄR	http://home6.swipnet.se/~w-60640/d2macnewz.htm	Porno-sites Video-butik	Intet	

Noter

[1] Jf. bemærkningerne til loven.

[2] Denne udlægning bygger på en samtale med Advokat Helge Olav Bergan, Oslo.

[3] Jf. bemærkningerne til det danske lovforslag.

[4] Advokat Helge Olav Bergan, Oslo.

[5]David Würgler varetager som kontaktperson for STOP både Canal Digitals og ViaSats interesser i forbindelse med piratkiggeri.http://www.stop.dk/index2.htm.

[6] Interview med David Würgler, STOP.

[7] Access systemer i digital tv er meget komplicerede, og alene hemmeligholdelse af informationer gør det svært at kortlægge alle dele af systemet.

[8] En tilfældig-tal-generator kan f.eks. være en maskine, som omsætter termisk støj af nogle elektriske komponenter til en talsekvens. Her gælder, at selv hvis man har fat i tro kopi af sådan en maskine kan man ikke gen-generere talsekvensen, da støjen er arbitrær og afhænger af mange parametre.

[9] Center for Tele-information: DVB - Fremtidens TV (Rapport til Kulturministeriet Juli 1998).

[10] Operatører af CA systemer, som f.eks. Telenor (Conax) hemmeligholder alle de vitale og følsomme oplysninger om deres system. Ved at ringe til SF Vision i Danmark, som ejes af Telenor, bliver man henvist til hovedkontoret i Norge for at få simple og uskadelige information om deres CA system.

[11] I en artikel i Berlingske Tidende d. 26.12.1998 er det ifølge Canal Digitals tekniske direktør Jens Thorsen ikke realistisk at adgangskoderne til de digitale tv-systemer bliver knækket indenfor en overskuelig fremtid. Skulle det mod forventningen alligevel lykkes, er Canal Digital i stand til flere gange dagligt at opdatere krypteringen således at det bliver nødvendigt for piraterne konstant at udskifte deres uautoriserede smartcards.

[12] Vilstrup Analyse december 1997 om udbredelsen af pirat-dekoderkort.