

LAUSUNTO ASIASSA R07/1004

Kai Puolamäki
Tietotekniikan osasto
PL 5400
02015 TKK
Kai.Puolamaki@tkk.fi
p. (09) 451 4482
f. (09) 451 3277

OLEN väitellyt vuonna 2001 filosofian tohtoriksi Helsingin yliopistosta teoreettisesta fyysikasta. Tämän jälkeen olen työskennellyt opettavan tutkijan virassa Teknillisen korkeakoulun Tietotekniikan osastolla. Opetus- ja tutkimusalani on informaatiotekniikka. En ole asianosaisten sukulainen, eikä minulla ole asiassa taloudellista intressiä.

VASTAAJIEN pyynnöstä lausun hovioikeudelle seuraavaa asiassa R07/1004:

1 Johdanto ja yhteenveto

ESITÄN tässä kappaleessa yhteenvedon CSS-suojauksen toimintaperiaatteesta ja taustasta, CSS:n tehokkuudesta ja julkisuudesta sekä vastaajien kirjoittamasta ohjelmasta. Seuraavissa kappaleissa käsittelen yksityiskohtaisemmin Holmanin lausuntoa (kappale 2), CSS:n julkisuutta (kappale 3), väitetyjä DVD CCA:n lisensoimia Linux-sovelluksia (kappale 4) sekä vastaajien ohjelmaa (kappale 5).

CSS:n toimintaperiaate. Nykyään useimmat DVD-elokuvat on talletettu DVD-levyille elokuvatiedostona, joka on salattu niin sanotulla CSS (Content Scramble System) -menetelmällä. Jotta tällaisen DVD-elokuvan voisi katella tietokoneella, pitää elokuvan katseluohjelman ensin autentikoida itsensä tietokoneen DVD-aseman kanssa. Tämän jälkeen katseluohjelman pitää muun muassa pystyä muuntamaan DVD-levyllä oleva elokuvatiedosto salatausta muodosta salaamattomaan, näytettävään muotoon. Tätä muunnosta kutsutaan ”salauksen purkamiseksi”. Salauksen purkamiseksi pitää tietää tai arvata salausavain, jota elokuvan salaamiseen on käytetty, tai salausmenetelmän heikkouksia hyväksi käyttäen muuten kiertää salaus.

CSS:n tausta. CSS-menetelmän alkuperäisiä kehittäjiä edustava yhdysvaltalainen DVD Copy Control Association (DVD CCA) on ilmoituksensa mukaan vuodesta 1998 alkaen lisensoinut erästä salauksen purkamiseen soveltuva ohjelmistoa ja dokumentaatiota. DVD CCA:n lisenssi vaatii järjestön ilmoituksen mukaan muun muassa salassapitosopimuksen allekirjoittamista. DVD CCA:n lisensoiman ohjelmiston lisäksi vuodesta 1999 alkaen on ollut tarjolla lukuisia kolmansien osapuolten itsenäisesti tekemiä ja vapaasti levittämiä DVD CCA:sta riippumattomia ohjelmistoja. Esimerkkejä tällaisista ohjelmista ovat DVD-elokuvien katseluun soveltuvat mediasoitinohjelmat VLC ja MPlayer sekä CSS:n purkuohjelman sisältävä libdvdcss. Nämä ohjelmat ovat vapaasti ja helposti saatavana muun muassa Microsoft Windows, Applen Mac OS X ja Linux-käyttöjärjestelmille. Nämä ohjelmat on saatavana myös ohjelmointitaitoisien helposti tutkittavissa olevassa lähdekoodimuodossa, jonka avulla jokainen voi tutustua CSS:n toimintaperiaatteisiin, luonnollisestikin ilman salassapitosopimusten allekirjoittamista.

CSS:n tekninen tehokkuus ja julkisuus. DVD CCA on pyrkinyt pitämään CSS:n toimintaperiaatteen salaisuutena. 16-vuotias norjalainen nuorukainen sai kuitenkin selville erästä soitinohjelmaa tutkimalla CSS:n toimintaperiaatteen, jonka hän julkaisi vuonna 1999. CSS:n toimintaperiaatteen pitäminen salaisena oli tärkeä tekijä CSS:n väitetyille tehokkuudelle. Vuodesta 1999 alkaen CSS:n toimintaperiaate on ollut yleisesti tiedossa ja se on sittemmin julkaistu useassa helposti saatavassa lähteessä, mukaanlukien yliopistojen opetusmateriaaleissa. DVD CCA luopui vuonna 2004 CSS-ohjelmia levittäneitä vastaan nostamistaan oikeusjutuista kalifornialaisen tuomioistuinten todettua, että CSS ei ole liikesalaisuus. Jokainen, jolla on riittävät ohjelmointitaidot DVD-soitinohjelman tekemiseksi, osaa julkisen dokumentaation avulla myös tehdä soitinohjelmassa tarvittavan CSS-salauksen kiertävän osan. CSS-salaus ei siis ole tehokas ainakaan teknisellä kriteerillä, koska kuka tahansa ylipäätään tarpeelliset ohjelmointitaidot omaava voi tehdä CSS-salauksen purkavan sovelluksen.

CSS:n tehokkuus ”loppukäyttäjän” näkökulmasta. DVD CCA:n lisensoimia soitinohjelmia on helposti saatavana muun muassa Microsoft Windows -käyttöjärjestelmään ja Applen Mac OS X -käyttöjärjestelmään. Monille muille käyttöjärjestelmille, joista Linux on tunnetuin, ei DVD CCA:n lisensoimia ohjelmia ole käytännössä tai helposti saatavana. DVD CCA on ilmoituksensa mukaan lisensoinut joitakin Linux-sovelluksia. Allekirjoittanut ei kuitenkaan onnistunut löytämään loppukäyttäjän ladattavissa olevaa erillistä soitto-ohjelmaa Suomessa yleisille Linux-jakeluille. Muille Linuxin kaltaisille käyttöjärjestelmille, joista voidaan mainita esimerkiksi FreeBSD, NetBSD ja

OpenBSD, ei DVD CCA tietääkseni edes väitä lisensoineensa yhtään mitään. Käytännössä tavallisen loppukäyttäjän, joka haluaa katsoa DVD-elokuvia Linuxilla tai Linuxin kaltaisella käyttöjärjestelmällä, tulee siis asentaa jokin DVD CCA:sta riippumaton ohjelmisto. Esimerkiksi DVD:n katseluun kykenevien DVD CCA:sta riippumattomien VLC-, MPlayer- tai libdvcss-ohjelmistojen asentaminen on loppukäyttäjille yhtä vaivatonta kuin minkä tahansa muun ohjelman asentaminen. Ohjelmien asentamisen jälkeen DVD-elokuvien katselu onnistuu normaalisti, vaikka DVD CCA:n lisensoimaa soitto-ohjelmaa ei olisikaan saatavana. Loppukäyttäjän, jollaisia lienee satoja tuhansia ellei miljoonia, näkökulmasta näiden tai muiden niiden kaltaisten ohjelmien asentaminen ja käyttö ei yleensä eroa muiden ohjelmien asentamisesta tai käytöstä, eikä loppukäyttäjä ohjelmia asentaessaan tai käyttäessään tyypillisesti miellä ”kiertävänsä” mitään suojausta tai ylipäätään huomaa CSS:n olemassaoloa mitenkään.

Vastaaajien Haskell-ohjelma. Vastaaajien julkaisema Haskell-ohjelmointikielillä kirjoitettu ohjelma sisältää lähdekoodimuotoisen kuvauksen CSS-suojatun elokuvatiedoston salauksen purkavasta osasta. Vastaaajien julkaisema ohjelma ei sisällä mitään sellaista uutta, joka ei olisi ollut julkista tietoa jo vuodesta 1999. Vastaaajien julkaisemasta ohjelmasta puuttuu suojauksen kiertämiseen tarvittava avain, joten ohjelma ei sellaisenaan pura elokuvatiedoston CSS-suojausta, eikä vastaaajien ohjelmaa siten voi käyttää CSS-suojauksen purkamiseen. Vastaaajien ohjelma ei sisällä DVD-aseman ja DVD:n soitto-ohjelman välistä autentikointia. Vastaaajien ohjelma siis ainoastaan purkaa DVD-elokuvatiedoston salauksen, jos käyttäjällä jo pääsy salattuun elokuvatiedostoon ja käyttäjä tietää salausavaimen. Vastaaajien ohjelmaa ei voi käyttää helpottamaan elokuvatiedoston kopiointia, vaan vastaaajien ohjelman kaltainen on tarpeen lähinnä elokuvan katselua varten, koska kopion voi yhtä hyvin tehdä niin salatusta kuin salaamattomastakin elokuvatiedostosta.

KÄSITTELEN seuraavissa kappaleissa eräitä edellä mainittuja asioita yksityiskohtaisemmin.

2 Holmanin lausunto

MINULLA oli tätä kirjoittaessani käytössäni kopio syyttäjän hovioikeuteen toimittamasta Futurmatix-nimisen yrityksen toimitusjohtaja Lindsay Holmanin englanninkielisestä lausunnosta. Verkkosivujensa mukaan (<http://www.futurmatix.com/service.htm>, tarkastettu 26.9.2007) Futurmatix harjoittaa kaupallista konsultointitoimintaa muun muassa teknisten

suojausten alalla.

Holmanin lausunnossa luetellaan paljon teknisiä yksityiskohtia, mutta jätetään mainitsematta lausuttavan asian kannalta keskeisiä seikkoja, sekä esitetään perusteettomia ja harhaanjohtavia väitteitä. Holmanin lausunto voi olla hyvä kuvaus kahdeksan vuotta sitten vallinneesta tilanteesta, mutta ei nykyhetkestä.

HOLMANIN lausunnossa painotetaan, että nimenomaan se, että CSS:n toimintaperiaate on salaisuus, on tärkeä seikka suojauksen tehokkuudelle. Lausunnossa kuvataan yksityiskohtaisesti lisenssin saajille asetettuja salassapitovaatimuksia.

Holmanin lausunnossa ei kuitenkaan mainita, että Linux-DVD-soittimen tekemiseksi tarvittava tieto CSS:n toimintaperiaatteista on ollut julkinen jo vuonna 1999. Näitä CSS:n toimintaperiaatteita on sen jälkeen opetettu yliopistojen luennoilla. Tämä seikka olisi mielestäni ehdottomasti tullut mainita Holmanin liikesalaisuuksia korostaneessa lausunnossa, jossa päinvastoin kerrotaan kuinka CSS:n toimintaperiaatteiden salaisuus luo ”suojakerroksen”, jota ei siis oikeasti ole olemassa. CSS:n julkisuutta käsitellään yksityiskohtaisemmin luvussa 3.

LAUSUNNOSSA viitataan liikesalaisuuksien lisäksi seitsemään patenttiin. Patenteja, joiden numeroita Holman ei mainitse ja joiden sisältöä en siten voi kommentoida, ei liene tämän asian kannalta merkitystä, enkä kommentoi niitä muuten kuin toteamalla, että patentit ovat julkisia dokumentteja ja siten patentissa kerrottu ei voi olla liikesalaisuus. Lisäksi totean, että kuka tahansa voisi tehdä vastaajien julkaiseman Haskell-koodin kaltaisen ohjelman julkaisutun helposti saatavilla olevan tiedon perusteella, tarvitsematta allekirjoittaa DVD CCA:n salassapitosopimuksia tai tutustua DVD CCA:n väitettyihin patentteihin.

HOLMANIN lausunnossa kuvataan CSS:n käyttämää salausjärjestelmää. Lausunnossa ei mainita siitä, että CSS on salausjärjestelmänä alla kuvatulla tavalla teknisesti heikko ja että CSS sisältää suunnitteluvirheitä.

CSS, kuten moni muukin salausjärjestelmä, perustuu siihen, että jotta esimerkiksi soitinohjelma voi purkaa salauksen, pitää soitinohjelman salausjärjestelmän toimintaperiaatteen lisäksi tuntea *avain*. Kuten Holmanin lausunnossa oikein sanotaan, avain on CSS:n tapauksessa 40-bittinen eli oleellisesti jokin positiivinen kokonaisluku väliltä $1-2^{40}$. 2^{40} on suuruudeltaan noin biljoona (1.000.000.000.000). Salauksen voi purkaa, jos tietää oikean avaimen eli kokonaisluvun. CSS:n tapauksessa mahdollisia avaimia on niin vähän, että jopa nykyiset kotitietokoneet voivat käydä kaikki mahdolliset avaimet läpi ja

siten arvaamalla löytää oikean avaimen — tietokoneelle 2^{40} ei lopultakaan ole kovin suuri luku. CSS:ssä olevien suunnitteluvirheiden vuoksi ei sitä paitsi edes ole tarpeen käydä kaikkia 2^{40} mahdollista avainta läpi, vaan oikea avain voidaan löytää sekunneissa. Kuvaus CSS:n toimintaperiaatteista ja suunnitteluvirheistä annetaan Carnegie Mellonin yliopistossa vuonna 2000 pidetyssä luennossa (luentomateriaali, mukaanlukien CSS:n toiminnan kuvaus, on saatavana osoitteessa

<http://www.cs.cmu.edu/~dst/DeCSS/Kesden/index.html>,

tarkastettu 26.9.2007; CSS:n toimintaa kuvataan myös artikkelissa Becker & Desosky, 2004. A Study of the DVD Content Scrambling System (CSS) Algorithm, In Proc 4th IEEE International Symposium on Signal Processing and Information Technology.).

DVD CCA:sta riippumattomia CSS:n purkamiseen pystyviä ohjelmia on saatavana runsaasti ja ne ovat helppoja käyttää ja asentaa. Nämä ohjelmat pystyvät purkamaan CSS-suojauksen, mikä on tarpeen DVD-elokuvan katselemista varten.

Holmanin väite, että CSS nykyään merkittävästi hidastaisi esimerkiksi elokuvien päätymistä ilman oikeudenhaltijan suostumusta tapahtuvaan Internet-levitykseen, on virheellinen ja perusteeton. Elokuvan luvattomaan Internet-levitykseen päätymiseen riittää, että *yksikin* levitykseen osallistuva pystyy suojauksen kiertämään ja tekemään suojaamattoman elokuvakopion.

DVD CCA on luopunut oikeustoimista riippumattomien CSS:n purkamiseen pystyvien ohjelmien levittäjiä vastaan. DVD CCA:n tosiasiallinen tarkoitus lieneekin nykyään lähinnä kerätä lisenssituloja fyysisistä DVD-soittimista ja tietokoneiden soitto-ohjelmista uusia väitetysti tehokkaampia suojausjärjestelmiä odoteltaessa.

CSS-suojauksen yksi osa on tietokoneen DVD-aseman ja DVD:n soitto-ohjelman välinen autentikointi, mukaanlukien elokuvamarkkinoiden alueelliseen jakamiseen tarkoitettut aluekoodit. Luultavasti nimenomaan nämä fyysiset soittolaitteet (sekä erilliset soittimet että tietokoneiden DVD-asemat) ovat DVD CCA:lle merkittävämpi lisensointikohde kuin henkilökohtaisissa tietokoneissa toimivat DVD-soitto-ohjelmat. Vastaaajien julkaisema ohjelmakoodi ei liity fyysisiin soittolaitteisiin.

HOLMAN myös lausuu, että DVD CCA on antanut kahdelle yritykselle (Sigma Designs ja InterVideo) lisenssin Linux-DVD-soitinta varten. Väite on harhaanjohtava: yrityksille on ehkä myönnetty lisenssi, mutta kuten jäljempänä kappaleessa 4 todetaan, kummankaan yrityksen tuotevalikoimasta en löytänyt tavallisen käyttäjän ladattavissa olevaa erillistä Linux-DVD-soitto-ohjelmaa.

JOHTOPÄÄTELMISSÄÄN Holman toteaa ”selvästi ja kiistattomasti”, mutta mitenkään perustelematta, että DVD-levyjen menestyksekkäs myynti johtuisi nimenomaan siitä, että CSS-suojaus estää kopioinnin. Hän käyttää tätä perusteena sille, että CSS olisi ”tehokas”. Holmanin väite on outo kahdesta syystä: (i) esimerkiksi musiikkia on myyty menestyksekkäästi digitaalisessa muodossa yli kymmenen vuotta CD-levyillä, joilla ei ole teknistä suojausta. Päinvastoin voidaan väittää, että suojausten puuttuminen on auttanut CD-levyjen menestystä, koska se on mahdollistanut muun muassa musiikin helpon kopioinnin kannettaviin soittimiin tavoilla, joita CD-formaatin suunnittelijat eivät osanneet ennakoida. Tekninen suojaus ei siis ole tarpeen sille, että mediaformaatti on menestyksekkäs — CD-formaatti on tästä esimerkki. (ii) Toisaalta CSS on helposti kierrettävissä. CSS:n avulla suojatut DVD-elokuvat löytävätkin tiensä nopeasti ilman oikeudenhaltijan lupaa tapahtuvaan Internet-levitykseen, johon riittää että yksikin potentiaalinen levittäjä voi suojausten murtaa. CSS:n tapauksessa jopa ohjelmointiin ja tietokoneen toimintaan perehtymätön ”tavallinen kuluttaja” voi tehdä DVD-elokuvista kopioita, kunhan hän hänellä on käytössään jokin tarvittavista helposti saatavista ja asennettavista ohjelmista.

3 CSS:n julkisuus

NORJALAINEN tuolloin lukiolainen Jon Lech Johansen selvitti erästä DVD CCA:n lisensoimaa soitto-ohjelmaa tutkimalla CSS:n toimintaperiaatteen. Hän julkaisi löydöksensä Internetissä vuonna 1999.

Tämän jälkeen on tehty lukuisia DVD CCA:sta riippumattomia CSS:n purkavimiseen pystyviä ohjelmistoja. Näitä ohjelmia on saatavana muun muassa Microsoft Windows, Applen Mac OS X ja Linux-käyttöjärjestelmille. Näitä ohjelmia jaetaan paitsi helposti asennettavassa muodossa myös lähdekoodimuodossa. Lähdekoodi on ohjelman muoto, jota sekä ihminen että tietokone voi ymmärtää. Yleensä ohjelmat kirjoitetaan lähdekoodimuodossa ja ”käännetään” ennen käyttöä tietokoneen nopeammin ymmärtämään muotoon. Lähdekoodia tutkimalla voi tutustua CSS:n toimintaperiaatteen. Tietojenkäsittelyn alalla lähdekoodi on usein paras dokumentaation muoto, koska se sisältää täsmällisen kuvauksen ohjelman toiminnasta.

Vastaajan julkaiseman CSS-salauksen purkavan ohjelman kaltaista lähdekoodia on painettu T-paitoihin, kahvikuppeihin ja jopa kravaatteihin. Katava kokoelma löytyy osoitteesta <http://www.cs.cmu.edu/~dst/DeCSS/Gallery/> (tarkastettu 26.9.2007). Suurin osa näistä julkaisuista keskittyy vuoden 2000 tienoille, jolloin aihe oli ajan-

kohtainen Yhdysvalloissa. CSS-lähdekoodia on julkaistu sadoissa ellei tuhansissa eri muodoissa ja lukemattomilla erilaisilla foorumeilla.

Harvardin yliopiston sivulla

<http://cyber.law.harvard.edu/openlaw/DVD/DeCSS/> (tarkastettu 26.9.2007) luetellaan lisää tapoja, joilla CSS:n toimintaperiaatteesta on julkisuudessa kerrottu.

Helsingin käräjäoikeuden kansliasta saa käsittääkseni pyynnöstä kopion oikeudenkäyntimateriaalin liitteenä olleesta vastaajan tekemästä CSS-salauksen purkavasta ohjelmasta.

Johansenin jälkeen CSS:n toimintaperiaatteita on analysoitu. Eräs mielenkiintoinen kuvaus CSS:n toiminnasta ja sen heikkouksista annetaan Carnegie Mellonin yliopistossa vuonna 2000 pidetyssä luennossa (luentomateriaali, mukaanlukien CSS:n toiminnan kuvaus, on saatavana osoitteessa <http://www.cs.cmu.edu/~dst/DeCSS/Kesden/index.html>, tarkastettu 26.9.2007; CSS:n toimintaa kuvataan myös artikkelissa Becker & Desosky, 2004. A Study of the DVD Content Scrambling System (CSS) Algorithm. In Proc 4th IEEE International Symposium on Signal Processing and Information Technology.). Mainituissa lähteissä kuvataan muun muassa CSS:n suunnitteluvirheitä.

Kalifornialainen tuomioistuin totesi vuonna 2004, että käytettävissä olevien tietojen mukaan laajalti julkaistu CSS:n toimintaperiaate ei voi olla liikesalaisuus (DVD CCA vs. Andrew Bunner). DVD CCA luopuikin Yhdysvalloissa vuonna 2004 kaikista muun muassa CSS-salauksen purkamiseen pystyvien ohjelmien levittäjiä vastaan nostamistaan kanteista.

4 DVD CCA:n lisensoima CSS Linuxin kaltaisessa käyttöjärjestelmässä

LINUXILLA tarkoitetaan arkikielessä usein oikeasti laaja perhettä käyttöjärjestelmäjakeluja, joille on yhteistä, että ne käyttävät Linux-ydintä. Suomessa yleisesti käytettyjä Linux-käyttöjärjestelmäjakeluja ovat — joitakin esimerkkejä mainitakseni — esimerkiksi Ubuntu GNU/Linux ja SUSE Linux. Linuxin lisäksi on olemassa Linuxin kaltaisesta vapaasti levitettäviä mutta eri ytimellä varustettuja käyttöjärjestelmäjakeluja, kuten FreeBSD, NetBSD ja OpenBSD.

Helposti asennettavat ja käytettävät käyttöjärjestelmäjakelut, kuten Ubuntu GNU/Linux, ovat mahdollistaneet sen, että Linux ei enää ole vain tietokoneharrastajille. Ubuntu kaltaiset käyttöjärjestelmäjakelut ovat monessa mielessä esimerkiksi Microsoftin Windows-käyttöjärjestelmää helppokäyttöi-

sempiä. Linux on nykyään suosittu vaihtoehto myös julkisella sektorilla, esimerkiksi kouluissa, joustavuutensa, helppokäyttöisyytensä ja edullisuutensa vuoksi.

Voidaan olettaa, että melkein kaikki Linuxilla DVD-elokuvia katsovat sadat tuhannet, elleivät miljoonat ihmiset, käyttävät aikaisemmin mainittujen kaltaista DVD CCA:sta riippumatonta CSS:n purkamiseen tarvittavaa ohjelmistoa.

HOLMAN sanoo lausunnossaan, että DVD CCA on lisensoinut soittimia Linux-käyttäjärjestelmälle. DVD CCA:n verkkosivulla <http://www.dvdcca.org/faq.html> (tarkastettu 26.9.2007) todetaan Linux-soittimista seuraavaa:

Can manufacturers of products for computers using the Linux operating system obtain a license to use CSS to manufacture a DVD player for Linux applications?

Absolutely. The DVD Copy Control Association would welcomes applications for the legal use of CSS from all manufacturers. In fact, Sigma Designs (www.sigmadesigns.com) is now marketing a DVD player for Linux under its license to manufacture products using CSS.

Menin DVD CCA:n neuvomalla tavalla Sigma Designs -yhtiön kotisivulle osoitteessa

<http://www.sigmadesigns.com/> (tarkastettu 26.9.2007). Products-linkki ("tuotteet") johti digitaalisista mediaprosessoreista kertoville sivuille osoitteessa

<http://www.sigmadesigns.com/public/Products/products.html> (tarkastettu 26.9.2007) Mainintaa Linuxilla toimivasta DVD-soitto-ohjelmasta en tältä tai muiltakaan yhtiön sivuilta löytänyt.

Verkkohaun avulla löysin PowerCinema Linux -nimisen ohjelmiston, joka ilmeisesti on DVD CCA:n lisensoima CyberLink-yhtiön jakelema ohjelma, joka on valmiiksi asennettuna japanilaiseen Suomessa marginaaliseen Turbolinux-käyttäjärjestelmäjakeluun. Yritin etsiä CyberLink-yhtiön kotisivuilta

<http://www.cyberlink.com/> (tarkastettu 26.9.2007) tätä tai muuta Linuxilla toimivaa soitto-ohjelmaa huonolla menestyksellä. Kaikki sivuilla mainitut DVD-soitto-ohjelmat (Cyberlink PowerDVD Ultra, PowerDVD, PowerCinema ja DVD Suite) vaativat Microsoft Windows -käyttäjärjestelmän (tarkastettu 26.9.2007).

Holmanin lausunnossa mainitaan myös InterVideo-yritys yhtenä Linux-soitto-ohjelmia tekevistä yrityksistä. Löysin yrityksen sivulta http://www.intervideo.com/jsp/Product_Profile.jsp?p=LinDVD (tarkastettu 26.9.2007) maininnan LinDVD-soitinohjelmasta, joka kuitenkin on saatavana yrityksen ilmoituksen mukaan vain valmistajille. Yksityishenkilöt eivät LinDVD:tä siis saa. Suomessakin jossain määrin käytetyn Mandrake-käyttäjärjestelmäjakelun yhteydessä LinDVD-soittimen voi ilmeisesti ostaa.

JOHTOPÄÄTÖKSENI on, että tyypillinen suomalainen Linux-käyttäjä ei saa tai ei ainakaan löydä Linux-käyttäjärjestelmälle erillisenä ohjelmana DVD CCA:n lisensoimaa DVD-soitto-ohjelmaa.

Tällainen soitto-ohjelma olisi luultavasti aina maksullinen jo pelkästään lisensointikulujen vuoksi. Loppukäyttäjän ei kannattaisi asentaa DVD CCA:n lisensoimaa maksullista soitinta, vaikka hän sellaisen jostain löytäisikin, koska helposti asennettavia ja käytettäviä DVD CCA:sta riippumattomia ilmaisia soitto-ohjelmia on saatavana lukuisia. Tästä syystä ei ole yllätys, että DVD CCA:n lisensoimaa Linux-soitinta ei löytynyt: taloudellista motivaatiota DVD CCA:n lisensoiman Linux-soittimen kehittämiseen, ylläpitoon ja markkinointiin ei ole, koska harva soitinta ostaisi.

Muille Linuxin kaltaisille käyttäjärjestelmille (mm. FreeBSD, NetBSD, OpenBSD) Holman ei edes väitä DVD CCA:n lisensoineen mitään.

5 Vastaaajien julkaisema ohjelma

KUTEN aikaisemmin mainittiin, kattava kokoelma vastaaajien julkaisemaa vastaavia ohjelmia on esitetty Carnegie Mellonin yliopiston sivulla <http://www.cs.cmu.edu/~dst/DeCSS/Gallery/> (tarkastettu 26.9.2007). Vastaaajien julkaisemaa vastaavia ohjelmia on julkaistu satoja ellei tuhansia.

Vastaaajien julkaisema ohjelma vaatii toimiakseen avaimen, joka on aikaisemmin kuvatulla tavalla $1-2^{40}$ väliltä oleva kokonaisluku. Vastaaajien ohjelma ei yritä arvata avainta tai edes käyttää CSS:n tunnettuja heikkouksia salauksen purkamiseen kaikkia avaimia läpikäymättä, vaan käyttäjän on annettava avain erikseen. Vastaaajien julkaisema ohjelma ei siis pura CSS-salausta, ellei ohjelman käyttäjä ennalta tiedä avainta, eikä ohjelmaa siten voi sellaisenaan käyttää CSS-salauksen kiertämiseen.

Vastaaajien ohjelma ei sisällä DVD-aseman ja DVD:n soitto-ohjelman välistä autentikointia. Vastaaajien ohjelma ainoastaan purkaa DVD-elokuvatiedoston salauksen, jos käyttäjällä on käytettävissään salattu elokuvatiedosto ja käyttäjä tietää salausavaimen. Vastaaajien ohjelmaa ei siis voi käyttää hel-

pottamaan elokuvatiedoston kopioimista, koska kopion voi yhtä hyvin tehdä niin salatusta kuin vastaajien ohjelman avulla salaamattomaksi muutetusta elokuvatiedostosta. Vastaajien ohjelman kaltainen onkin hyödyllinen lähinnä elokuvatiedoston sisältämän elokuvan katselua varten.

Kuten Holman oikein toteaa lausunnossaan salausta koskevassa kappaleessa: salausrjestelmät suunnitellaan olettaen, että mahdollinen vastapuoli tietää salausrjestelmän toimintaperiaatteen. Jos salausrjestelmä on tehokas, ei salausrjestelmän toimintaperiaatteen kuvaus täten helpota rjestelmän kiertämistä, vaan salausta ei voi kiertää ellei avain ole tiedossa. Käytössä olevat luotettavat salausrmenetelmät, kuten esimerkiksi verkkopankkiyhteyksien turvaamiseen käytetyt salausrmenetelmät, perustuvat julkisiin standardeihin. Salausrmenetelmien julkisuus tekee menetelmistä vahvempia ja luotettavampia, koska menetelmien mahdolliset heikkoudet on voitu julkisessa tarkastelussa havaita ja korjata. Kokemus on osoittanut, että jos salausrjestelmän tehokkuuden takaamiseksi rjestelmän toimintaperiaate pitää pysyä salaisuutena, ei rjestelmä oikeasti ole tehokas (ks. esim. Schneier, 1996. *Applied Cryptography*, 2nd ed. John Wiley & Sons, s. 7–8).

Vastaajat ovat nimenomaan tässä tapauksessa pelkästään kuvanneet julkaisemallaan ohjelmakoodilla CSS-rjestelmän erään osan toimintaperiaatteen. Jos CSS olisi tehokas, ei tällainen pelkkä toimintaperiaatteen kuvaus siis voisi helpottaa ”suojuuksen kiertämistä”.

Kukaan tuskin käyttäisi tai kehittäisi edelleen vastaajien julkaisemaa ohjelmaa, koska ohjelma ei sellaisenaan ole käyttökelpoinen eikä Haskell-kieltä yleensä käytetä DVD:n soittamiseen. Paljon parempia sovelluksia on helposti ja ilmaiseksi saatavana.


Vastaajien julkaisema ohjelma on merkityksellinen lähinnä CSS:n toimintaperiaatteen kuvauksena. Vastaajien ohjelma on tyypillinen, joskaan ei kaikista selkein, Haskell-kielillä kirjoitettu esimerkki tietojenkäsittelytieteen opetuksessa ja tutkimuksessa käytetystä ohjelman toimintaperiaatteen kuvauksesta.

Johtopäätöksenä voidaan todeta, vastaajien julkaisema Haskell-kielinen ohjelma ei tuo tähän keskusteluun yhtään mitään uutta. Vastaajien tarkoituksena on tuskin ollut tehdä missään käytännön sovelluksessa toimivaa ohjelmaa.

TIETOJENKÄSITTELYTIEDESSÄ tietokoneohjelmat ovat keskeinen sovellus- ja tutkimusaihe. Tietojenkäsittelytieteessä vastaajien julkaiseman kaltainen lähdekoodi onkin keskeinen ilmaisun muoto. Esimerkiksi salausrjestelmien opetuksessa ja tutkimuksessa on tärkeää tutustua salausrjelmiin ja erityisesti niiden suunnittelussa tehtyihin virheisiin. Esimerkiksi CSS-suojuuksen toteutuksen puutteisiin tutustuminen on välttämätöntä, jotta opiskelijat voi-

vat valmistuttuaan välttää samanlaiset virheet. Tästä syystä on tärkeää, että tietojenkäsittelyn tutkijat ja opiskelijat voivat tutustua vastaajien kirjoittaman kaltaisiin ohjelmiin. Varsinkin kun otetaan huomioon, että vastaajien kirjoittama ohjelma on erittäin epäkäytännöllinen, näen että vastaajien kirjoittaman ohjelma on enemminkin osa tietojenkäsittelytieteen ”akateemista keskustelua”, jossa tärkeänä osana on CSS:n kaltaisten ohjelmien toiminnan täsmällinen lähdekoodimuotoinen, esimerkiksi Haskell-kielellä kirjoitettu, kuvaus.

Otaniemessä 21. marraskuuta 2007

A handwritten signature in blue ink, appearing to read 'Kai Puolamäki', on a light blue background.

Kai Puolamäki