

Lausunto liittyen Helsingin hovioikeuden 22.5.2008 antamaan tuomioon nro 1427 (diaarinro R 07/2622)

Asia: Teknisen toimenpiteen loukkausrikkomus

Lausunnon pyytäjä: Oikeustieteen kandidaatti Mikko Välimäki

Lausunnon antaja: Diplomi-insinööri Arto Teräs

Vastaan Mikko Välimäen esittämiin kysymyksiin parhaan tietämykseni mukaisesti.

1. Lausunnon antajan tausta ja koulutus

Olen koulutukseltani tietotekniikan DI (Teknillinen korkeakoulu, 2004). Erikoisosaamistani ovat Linux/Unix-järjestelmät, avoimen lähdekoodin ohjelmistot sekä verkko- ja grid-teknologiat. Opintoihini kuului myös algoritmi- ja tietoturva-aiheisia kursseja. Olen toiminut Suomen Linux-käyttäjien yhdistys Finnish Linux User Group FLUG ry:ssä useissa eri luottamustehtävissä, mm. hallituksen jäsen ja tiedottaja 2001-2002, varapuheenjohtaja 2004, puheenjohtaja 2005, hallituksen jäsen ja tiedottaja 2008.

Olen tutustunut tuomioon, vastaajien Haskell-ohjelmakoodiin sekä CSS-algoritmin toimintaan.

2. Tekijänoikeudellisesti relevantti käyttö

(a) Voiko CSS-suojakeinoa tarkastella teknisesti vaiheina tai osina?

Kyllä. Olennaisesti CSS-suojauksessa on kaksi osaa: tunnistus (CSS authentication) ja salausta (CSS encryption). Ohjelman on tunnistauduttava DVD-aseman kanssa, ennen kuin DVD-levyltä voidaan lukea tietoa ulos. Sen jälkeen luetun tiedon saamiseksi nähtäville on avattava salausta.

Tunnistus on edelleen jaettu useampaan osaan, jossa suoritetaan melko moniportainen avainten vaihto.

(b) Ovatko kopioinnin esto ja katselemisen esto teknisesti erillisiä vaiheita?

Kyllä. Levyn sisältämät tiedostot voi kopioida tunnistuksen (CSS authentication) jälkeen, mutta niitä ei voi silti vielä katsella purkamatta salausta. Siten tunnistus on olennaisesti kopioinnin esto ja salausta (CSS encryption) katselemisen esto. Identtisten kopioiden tekeminen levyistä on lisäksi estetty siten, että normaalikäyttäjille myytävillä DVD-kirjoittimilla ei voida tallentaa DVD-R- tai DVD-RW-levyille CSS-suojauksen vaatimia piilosektoreita.

Suojauksen kaksivaiheisuus voidaan todentaa Linux-järjestelmässä toimivalla esimerkillä, joka on esitetty liitteessä 1.

(c) Edellyttäväkö kopiointieston kiertäminen katselueston kiertämistä?

Pelkkä materiaalin kopiointi ei edellytä katselueston kiertämistä.

Levyiltä voidaan kopioida sen sisältämät tiedostot CSS-tunnistuksen jälkeen avaamatta salausta, siirtää ne esimerkiksi tietoverkon välityksellä toiselle tietokoneelle, ja katsella elokuva ohjelmalla joka osaa avata salauksen.

(d) Kiertääkö vastaajien Haskell-ohjelmakoodi kopiointieston vai katselueston?

Vastaajien Haskell-koodi avaa CSS-salauksen eli kiertää katselueston. Se ei suorita CSS-tunnistusta. On tosin huomattava, että elokuvan katselemiseksi DVD-levyltä pitää suorittaa sekä CSS-tunnistus että salauksen avaus. Koodi ei siis sellaisenaan ole riittävä elokuvan katselemiseksi.

3. Suojakeinon tehokkuus

(a) Vaatiiko DVD-elokuvan katselu Linux-järjestelmissä aina välttämättä jonkun lisäohjelmiston asennuksen?

Ainakin pääsääntöisesti kyllä.

(b) Jos DVD-elokuvan katseluun vaaditaan jonkun lisäohjelmiston asennus, millaisesta ohjelmistosta on yleensä kysymys?

Ohjelmakirjastosta, joka toteuttaa CSS-tunnistuksen ja CSS-salauksen avauksen. Videoiden toisto-ohjelmat käyttävät kyseistä kirjastoa pystyäkseen näyttämään CSS-suojattuja levyjä. Toisto-ohjelma tulee usein mukana jo perusasennuksessa, mutta CSS-suojattujen levyjen katsomiseksi on yleensä haettava erikseen salauksen avaamiseen pystyvä kirjasto.

(c) Kuinka helppoa tälläisen ohjelmiston asennus on?

Varsin helppoa. Tyypillisesti käyttäjän on haettava paketti erikseen verkosta, mutta sen jälkeen asennus onnistuu yhdellä komennolla kuten muidenkin ohjelmien asentaminen.

Koska DVD-levyjen katsominen on suosittua, asennukseen löytyy helposti neuvoja. Esimerkiksi Google-haulla "Ubuntu dvd playback" tai suomeksi "Ubuntu dvd-toisto" löytää ohjeet nykyisin Suomessa kotikäytössä yleisimpään Linux-jakeluun, Ubuntuun. Ohjeet löytyvät myös Ubuntu Suomi -yhteisön kirjoittamasta "Ubuntu tutuksi" -nimisestä sähköisestä kirjasta, joka on suunnattu aloitteleville käyttäjille.

(d) Mieltääkö "tavallinen käyttäjä" tällöin asentavansa suojakeinon kierto-ohjelmiston?

Ei miellä. Hän mieltää asentavansa lisäpaketin, joka mahdollistaa dvd-levyjen katselun. Ohjeissa puhutaan nimenomaan levyjen katselusta, ei kopioinnista.

Asennusvaiheessa tai ohjeissa saatetaan mainita siitä, että ohjelmaa ei voida kaikkialla maailmassa levittää vapaasti. Mainittuja syitä ovat mm. U.S.A:n lait, CSS-patentit tai yleisemmin "licensing restrictions" tai "legal restrictions".

Tietokoneohjelmia asennettaessa tulee kaikissa yleisimmissä järjestelmissä (Windows, Mac, Linux) usein vastaan erilaisia varoituksia ja kieltoja, joten käyttäjät ovat tottuneet ohittamaan ne ilman tarkempaa pohtimista.

4. Haskell-koodin toimivuus?

(a) Toimiiiko vastaajien Haskell-ohjelmakoodi?

En ole kokeillut suorittaa ohjelmaa. Jo ohjelmakoodia katsomalla on kuitenkin havaittavissa, että se vaatii toimiakseen salausavaimen, jota ei toimiteta koodin mukana. Siten koodia ei voi sellaisenaan käyttää, ellei tiedä purettavan tiedoston salauksessa käytettyä avainta.

(b) Mikä vastaajien Haskell-ohjelmakoodin käyttötarkoitus on?

Ohjelmakoodin käyttötarkoitus on antaa tietoa CSS-salauksen toiminnasta.

Tähän käyttötarkoitukseen viittaa erityisesti kolme piirrettä:

- 1) Ohjelmointikielen valinta. Haskell-kieltä käytetään yleisimmin nimenomaan opetustarkoituksissa.
- 2) Ohjelmakoodi ei ole suoraan käyttökelpoinen. Koodi toteuttaa vain salauksen avauksen eli yhden osan CSS-suojauksesta, eikä jonkun tietyn kyseisellä menetelmällä salatun tiedoston (kuten DVD-elokuvan) avaamiseen tarvittavaa salausavainta toimiteta sen mukana.
- 3) Ohjelmakoodin esittäminen osana sitä selittävää tekstiä. Algoritmien havainnollistamiseksi käytetään ohjelmoinnin oppikirjoissa yleisesti tämän kaltaisia ohjelmakoodiesimerkkejä.

TKK:lla vuonna 2000 suorittamassani Tiedon salaus ja suojaus -kurssissa oli oppikirjana Applied Cryptography (Bruce Schneier, ISBN 0-471-11709-9), joka sisältää useiden eri salausmenetelmien purkamisen lähdekoodina. Vastaajien Haskell-ohjelmakoodi on hyvin samankaltainen kuin kirjan esimerkit.

5. Allekirjoitus

Helsingissä 2.7.2008

Arto Teräs

Liite 1. CSS-suojauksen toimintaa havainnollistava esimerkki.

Tässä esimerkissä havainnollistetaan, mitä tapahtuu yritettäessä kopioida Matrix-elokuvaa tietokoneen kiintolevylle. Esimerkissä on käytetty komentorivityökaluja, mutta kohdissa 4 ja 11 käytetyn kopiointikomennon (cp) sijaan voisi aivan yhtä hyvin käyttää graafista tiedostonhallintaohjelmaa. Vastaavasti kohdassa 7 käytetyn tstdvd-ohjelman sijaan voi katsoa elokuvaa hetken jollakin dvd-toisto-ohjelmalla, joka osaa suorittaa CSS-tunnistuksen.

Lihavoituna oleva teksti esittää käyttäjän kirjoittamia komentoja. Esimerkin kulku on seuraava:

1. Siirrytään kiintolevyltä sijaitsevaan hakemistoon /media/disk/dvd_testi.
 2. Listataan hakemiston sisältö. Hakemisto on tyhjä.
 3. Listataan dvd-levyllä hakemistossa /dvd/VIDEO_TS/ olevat videotiedostot. Elokuva koostuu näistä tiedostoista.
 4. Yritetään kopioida yksi tiedostoista (VTS_01_1.VOB) kiintolevylle normaalilla kopiointikomennolla (cp). Kopiointi epäonnistuu.
 5. Listataan hakemiston sisältö. Hakemistoon on ilmestynyt tiedosto VTS_01_1.VOB, jonka koko on kuitenkin nolla.
 6. Poistetaan nollakokoinen tiedosto.
 7. Aloitetaan alusta. Otetaan dvd-levy ulos asemasta ja laitetaan takaisin sisään. Suoritetaan CSS-tunnistus tstdvd-ohjelmalla.
 8. Listataan hakemiston sisältö. Tstdvd-ohjelma on tallentanut sinne tunnituksessa tarvittavan levyn avaimen (disc key). DVD-levyllä olevat tiedostot on edelleen salattu nimikeavaimilla (title key) ja sektoriavaimilla (sector key).
 9. Poistetaan levyn avain.
 10. Varmistetaan, että hakemisto on tyhjä.
 11. Yritetään kopioida tiedosto VTS_01_1.VOB kiintolevylle normaalilla kopiointikomennolla (cp), kuten kohdassa 4. Tällä kertaa kopiointi onnistuu.
 12. Listataan hakemiston sisältö. Hakemistoon on ilmestynyt tiedosto VTS_01_1.VOB, joka on samankokoinen kuin DVD-levyllä oleva vastaava tiedosto.
 13. Lasketaan tarkistussumma DVD-levyllä levyllä olevasta tiedostosta.
 14. Lasketaan tarkistussumma kiintolevyllä olevasta tiedostosta. Summa täsmää edellisessä kohdassa lasketun summan kanssa. Tiedosto on siis täsmälleen sama kuin DVD-levyllä oleva tiedosto, eli se sisältää edelleen salauksen.
- Levyn muut tiedostot voidaan kopioida vastaavasti. Komennolla **cp -a /dvd/* .** saadaan kopioitua kaikki tiedostot.

```
1. $ cd /media/disk/dvd_testi
```

```
2. /media/disk/dvd_testi$ ls -la
total 8
drwxr-xr-x  2 arto root 4096 Jun 30 23:29 .
drwxr-xr-x 18 root root 4096 Jun 30 23:29 ..
```

```
3. /media/disk/dvd_testi$ ls -la /dvd/VIDEO_TS/*.VOB
-r--r--r--  1 4294967295 4294967295   1087488 Oct 16 1999 /dvd/VIDEO_TS/VIDEO_TS.VOB
-r--r--r--  1 4294967295 4294967295         0 Oct 16 1999 /dvd/VIDEO_TS/VTS_01_0.VOB
-r--r--r--  1 4294967295 4294967295  879589376 Oct 16 1999 /dvd/VIDEO_TS/VTS_01_1.VOB
```

```

-r--r--r-- 1 4294967295 4294967295 115369984 Oct 16 1999 /dvd/VIDEO_TS/VTS_02_0.VOB
-r--r--r-- 1 4294967295 4294967295 1073739776 Oct 16 1999 /dvd/VIDEO_TS/VTS_02_1.VOB
-r--r--r-- 1 4294967295 4294967295 1073739776 Oct 16 1999 /dvd/VIDEO_TS/VTS_02_2.VOB
-r--r--r-- 1 4294967295 4294967295 305852416 Oct 16 1999 /dvd/VIDEO_TS/VTS_02_3.VOB
-r--r--r-- 1 4294967295 4294967295 1073739776 Oct 16 1999 /dvd/VIDEO_TS/VTS_02_4.VOB
-r--r--r-- 1 4294967295 4294967295 1073739776 Oct 16 1999 /dvd/VIDEO_TS/VTS_02_5.VOB
-r--r--r-- 1 4294967295 4294967295 965672960 Oct 16 1999 /dvd/VIDEO_TS/VTS_02_6.VOB
-r--r--r-- 1 4294967295 4294967295 0 Oct 16 1999 /dvd/VIDEO_TS/VTS_03_0.VOB
-r--r--r-- 1 4294967295 4294967295 1058738176 Oct 16 1999 /dvd/VIDEO_TS/VTS_03_1.VOB

```

```

4. /media/disk/dvd_testi$ cp /dvd/VIDEO_TS/VTS_01_1.VOB .
cp: reading `/dvd/VIDEO_TS/VTS_01_1.VOB': Input/output error

```

```

5. /media/disk/dvd_testi $ ls -la
total 8
drwxr-xr-x 2 arto root 4096 Jun 30 23:31 .
drwxr-xr-x 18 root root 4096 Jun 30 23:29 ..
-r--r--r-- 1 arto arto 0 Jun 30 23:31 VTS_01_1.VOB

```

```

6. /media/disk/dvd_testi$ rm -f VTS_01_1.VOB

```

```

7. /media/disk/dvd_testi$ /media/disk/css-auth/tstdvd /dev/dvd
not Authenticated
Request AGID [1]... AGID 0
Host sending challenge: 09 08 07 06 05 04 03 02 01 00
LU sent key1: B1 93 74 A2 3E
Drive Authentic - using variant 5
LU sent challenge: 62 67 CB 64 39 3D 7E 47 9B F2
Host sending key 2: 71 A3 5C 75 02
DVD is authenticated
Received Session Key: 00 6D 1E 18 64
not Authenticated
Received Disc Key: EA C5 81 F4 86 F3 3B 13 82 C8
Authenticated

```

```

8. /media/disk/dvd_testi$ ls -la
total 12
drwxr-xr-x 2 arto root 4096 Jun 30 23:33 .
drwxr-xr-x 18 root root 4096 Jun 30 23:29 ..
-rw-r--r-- 1 arto arto 2048 Jun 30 23:33 disk-key

```

```

9. /media/disk/dvd_testi$ rm disk-key

```

```

10. /media/disk/dvd_testi$ ls -la
total 8
drwxr-xr-x 2 arto root 4096 Jun 30 23:36 .
drwxr-xr-x 18 root root 4096 Jun 30 23:29 ..

```

```

11. /media/disk/dvd_testi$ cp /dvd/VIDEO_TS/VTS_01_1.VOB .

```

```

12. /media/disk/dvd_testi$ ls -la
total 859828
drwxr-xr-x 2 arto root 4096 Jun 30 23:36 .
drwxr-xr-x 18 root root 4096 Jun 30 23:29 ..
-r--r--r-- 1 arto arto 879589376 Jun 30 23:48 VTS_01_1.VOB

```

```

13. /media/disk/dvd_testi$ md5sum /dvd/VIDEO_TS/VTS_01_1.VOB
14e5e1bb0875ab90895acb9cbf9a35ea /dvd/VIDEO_TS/VTS_01_1.VOB

```

```

14. /media/disk/dvd_testi$ md5sum /media/disk/dvd_testi/VTS_01_1.VOB
14e5e1bb0875ab90895acb9cbf9a35ea /media/disk/dvd_testi/VTS_01_1.VOB

```