

Arkipäivän tietoturvaa: TrueCryptillä salaat kiintolevyn helposti

Artikkelin on kirjoittanut Otto Kekäläinen.

Edellisessä Turvallisuus-lehden numerossa käsiteltiin PDFCreator-ohjelman käyttöä salattujen PDF-tiedostojen tekoon ja 7-Zip-ohjelmaa salattujen pakettien tekoon. Seuraavaksi esitellään TrueCrypt-ohjelma, jolla voi tehdä salattuja tiedostosäilöjä sekä kokonaan salattuja USB-tikkuja ja kiintolevyjä.

Säilössä tiedot pysyy suojassa

Edellisessä artikkelissa kuvaamani salattujen zip-pakettien hyvä puoli on se, että salatut zip-paketit voi purkaa lähes missä tahansa tietokoneessa. Vastaanottajalla ei tarvitse olla täsmälleen samaa zip-ohjelmaa, koska tiedostomuoto on yleinen ja toimittajariippumaton. Salattujen zip-pakettien lähettämisessä kannattaa kuitenkin huomioida se, että sen jälkeen, kun vastaanottaja on purkanut paketin, löytyvät tiedostot salaamattomina tämän kiintolevyltä. Jos vastaanottajalla ei ole käytössä kiintolevysalausta, voidaan tiedostot kaivaa kiintolevyanalyysillä esiin jopa sen jälkeen, kun käyttäjä luulee poistaneensa ne.

Parasta olisi säilyttää salatut tiedostot kokoajan erityisessä säilössä, jossa tiedostot pysyvät koko ajan salattuna vaikka niitä avattaisiin ja muokattaisiin. Tällaisen säilön voi luoda TrueCryptillä.

TrueCryptillä luotu säilö on yleensä yksi tiedosto, jolle käyttäjä saa valita koon ja nimen. Kun säiliö avataan, ilmestyy tietokoneeseen virtuaalinen levyasema, jonne tiedostoja voi siirtää aivan kuten esimerkiksi muistitikulle.

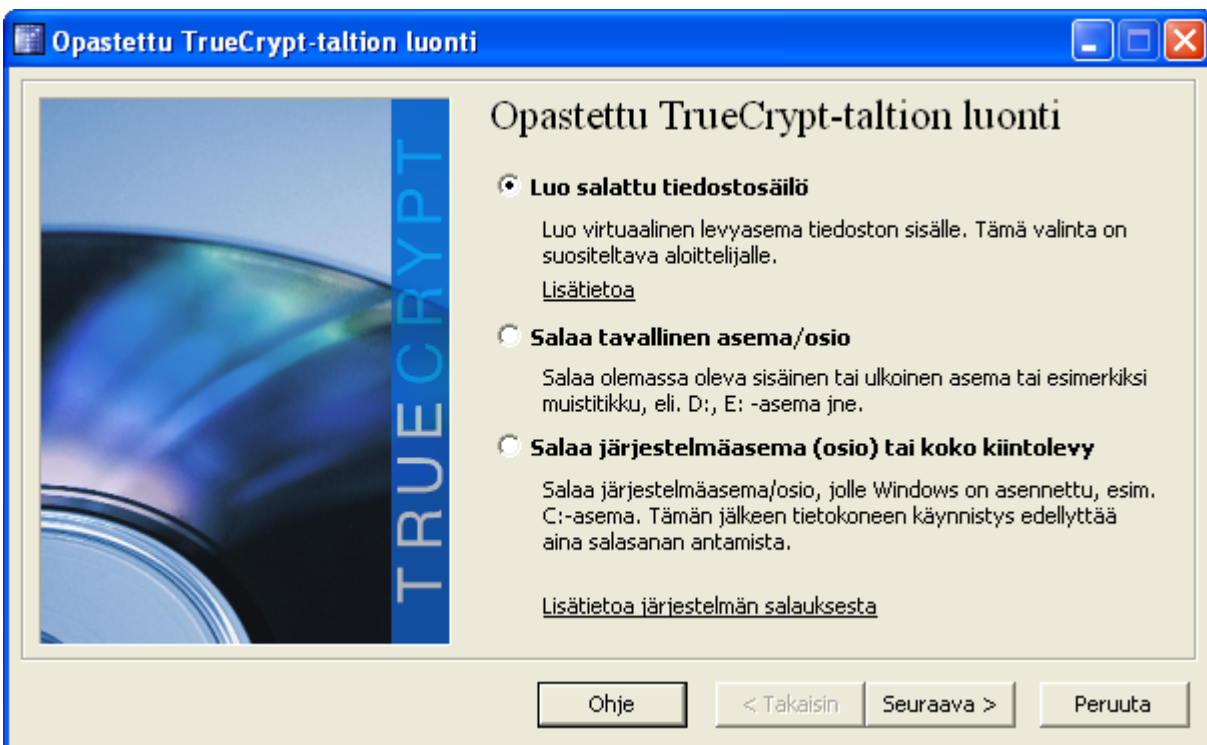
Esimerkiksi jos tietokoneessa on normaalisti vain C- ja D-asetat (kiintolevy ja CD/DVD-asema), tulee käyttöön E-asema kun salattu säilö avataan. Tällöin E-aseman kautta mikä tahansa ohjelma pääsee tiedostoihin käsiksi, aivan kuin ne olisivat normaaleja tiedostoja, vaikka todellisuudessa taustalla toimiva TrueCrypt purkaa ja salaa tiedostot ajon aikana. Näin tiedoista ei jää salaamattomia kopioita kiintolevylle.

Pienen säilön voi myös lähettää sähköpostitse, jolloin se salaa tiedot siirron aikana ja vastaanottajan levyllä. Liitetiedostojen kokorajoitus tulee kuitenkin muistaa. Säilön tiedostomuoto on kuitenkin TrueCryptiin sidonnainen, joten säilöjä lähetellessä pitää varmistua että vastaanottajallakin on TrueCrypt. Onneksi TrueCrypt on avointa lähdekoodia, eli ilmainen, ja se on saatavilla kaikille yleisille käyttöjärjestelmille.

TrueCryptin tiedostosäilön käyttö vaatii hieman suunnittelua. Luontivaiheessa säilölle täytyy määritellä mm. koko, esimerkiksi 10 megatavua. Koko on kiinteä eikä se kasva kun säilön sisään laitetaan tiedostoja. Jos säilöstä loppuu tila, täytyy luoda kokonaan uusi isompi säilö.

Suljettuna säilö näyttää miltä tahansa tiedostolta jonka nimi ja tiedostopääte voi olla mitä tahansa. Itse asiassa sisältö on rakennettu siten, että sitä analysoimalla ei voi edes

päätellä kyseessä olevan TrueCryptillä tehty salattu tiedostosäilö. Tiedostot pysyvät siis tarvittaessa sekä salassa että piilossa.



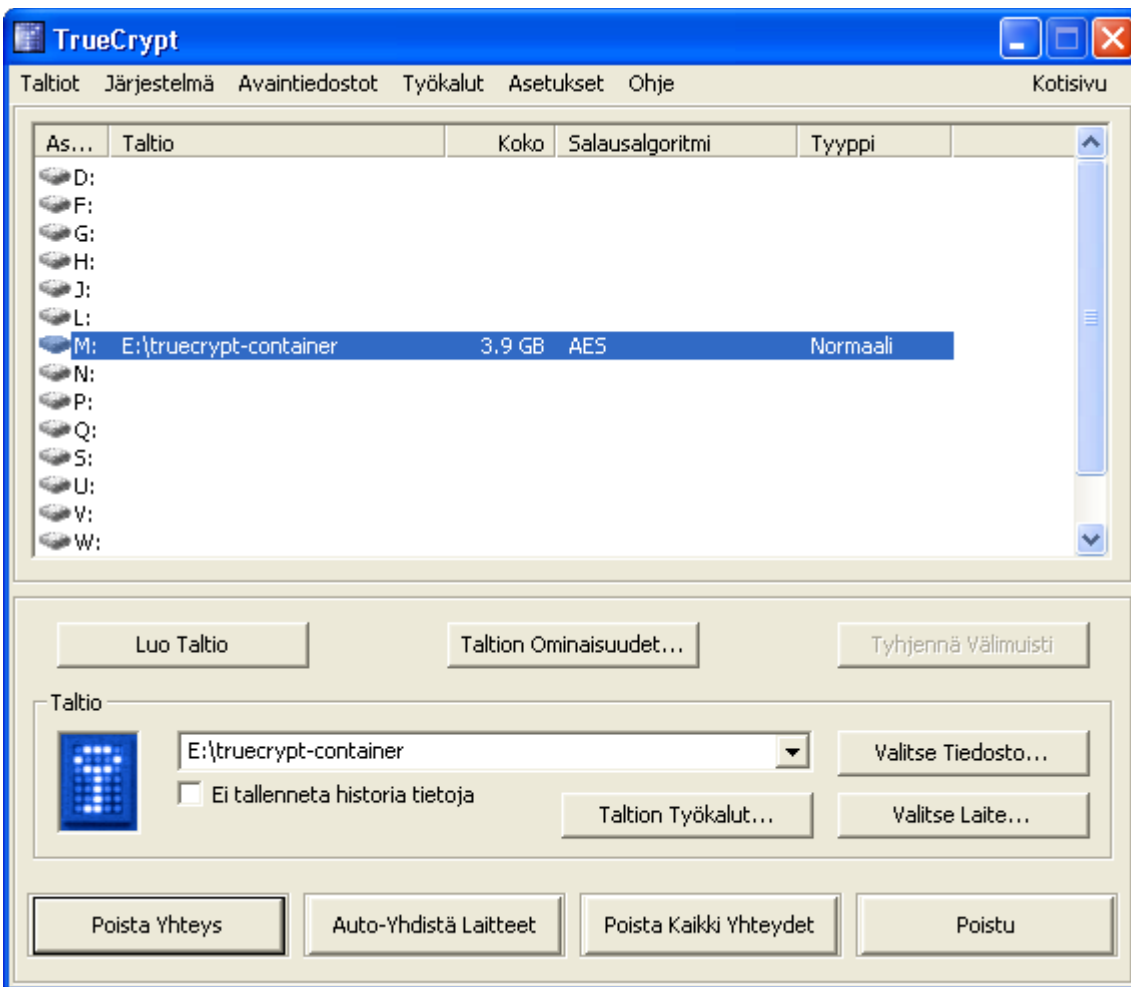
TrueCrypt-salausohjelmalla voi tehdä yksittäisiä säilöjä tiedostoina tai salata kokonaisia kiintolevyosioita. Salauksen toimivuuteen voi luottaa, koska TrueCryptin auditointiin on osallistunut mm. Bruce Schneier, maailmankuulu tietoturva-asiantuntija.

Lisäsuojaa säilön piilottamisella

TrueCryptissä on muutamia teknisesti hienoja lisäominaisuuksia, jotka liittyvät salauksen olemassaolon kiistämiseen (engl. plausible deniability). Säilön voi halutessaan luoda olemassa olevan tiedoston sisään, jolloin puhutaan steganografiasta. Esimerkiksi 100 megatavun säilön voisi piilottaa 600 megatavun elokuvatiedoston sisälle. Elokuvaa voi tämän jälkeen edelleen katsella normaalisti eikä tavallinen käyttäjä huomaa säilöä mitenkään. Säilön avaamiseen pitää siis tietää paitsi itse salasana, niin myös ylipäänsä missä tiedostossa säilö on.

Esimerkissä uuden elokuvatiedoston koko luonnollisesti kasvaa ja jos joku pääsee vertailemaan alkuperäistä ja uutta tiedostoa, voi niiden eroista päätellä steganografian käytön.

Lisäksi säilöihin voi tehdä eräänlaisen valepohjan: yhdellä salasanalla säilö aukeaa siten, että vain valetiedostot näkyvät, ja vasta toisella salasanalla koko säilö aukeaa kokonaan ja oikeasti suojattavat tiedostot näkyvät. TrueCryptin kehittäjä on ajatellut tämän ominaisuuden olevan hyödyllinen, jos käyttäjää kidutetaan paljastamaan salatun säilön salasanan. Tällöin kidutetun ei tarvitse antaa oikeaa salasanaa ja kiduttajat ovat tyytyväisiä kun uskovat saaneensa salauksen auki. Näistä hienouksista tuskin kuitenkaan on hyötyä arkikäyttäjälle.

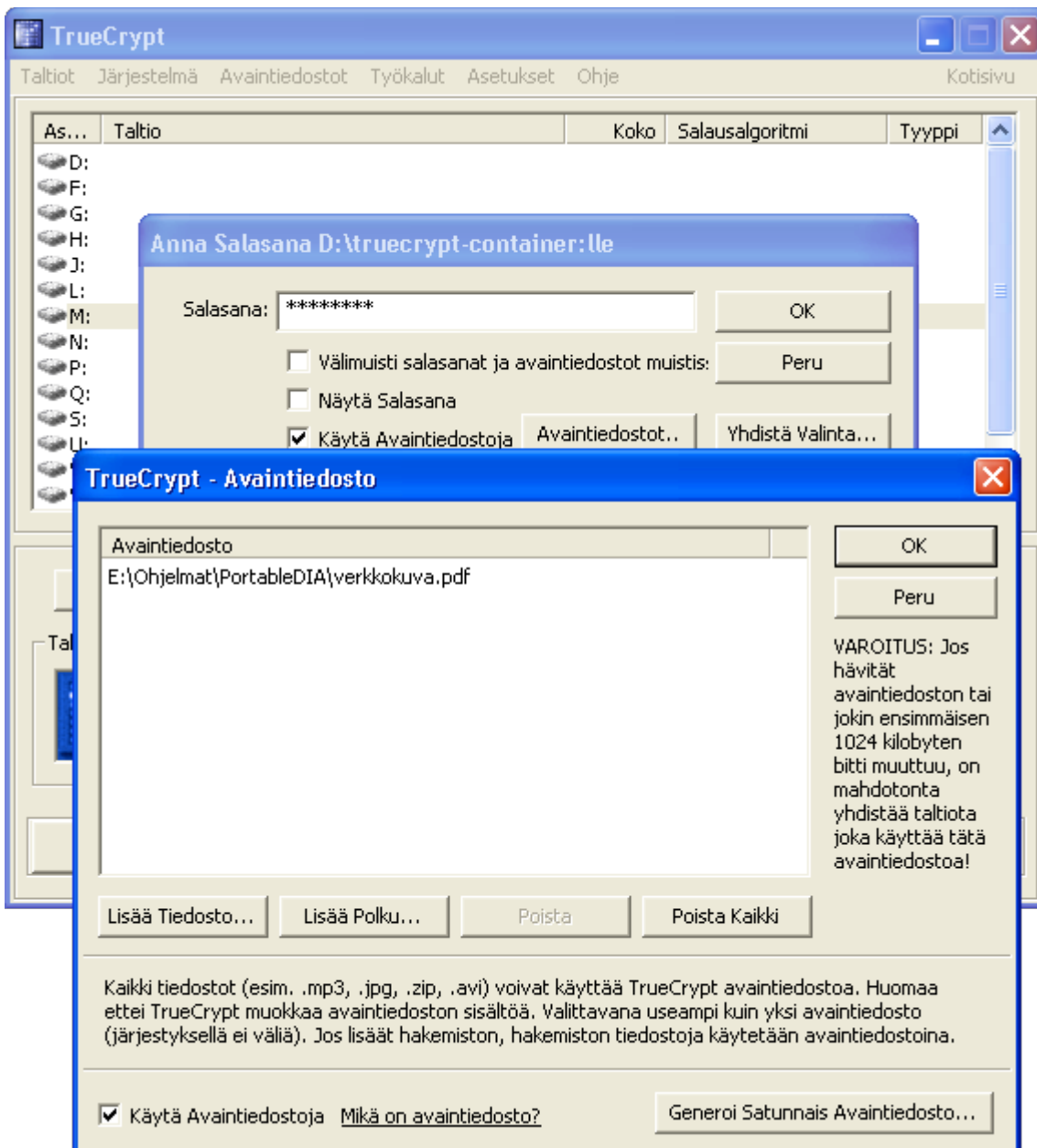


Avattuna säilö näkyy Windowsissa normaalina levyasemana, jossa olevia tiedostoja mikä tahansa ohjelma voi käsitellä. TrueCrypt hoitaa salauksen taustalla käyttäjän huomaamatta.

Koko kiintolevyn salaaminen

Tiedostoon sijoitettavan säilön lisäksi TrueCryptillä voi salata kokonaisia kiintolevyosioita tai muistitikkuja. Arkikäytössäkin kannattaa salata tietokoneen kiintolevy. Varsinkin kannettava tietokone voi joutua helposti varkauden uhriksi ja silloin helpottaa, jos varkaalle on menettänyt pelkästään laitteen eikä sen sisällä olleita sähköposteja, asiakirjoja, valokuvia ja muita mahdollisesti yksityisiä tai luottamuksellisia tietoja. Myös USB-tikut ja ulkoiset kiintolevyt kannattaa salata samasta syystä. Muista myös varmuuskopiot – siltä varalta että kiintolevy varastetaan tai unohdat salasanan etkä pääse enää tietoihin käsiksi, kannattaa etukäteen laittaa tärkeät tiedot varalevylle kassakaappiin tai vastaavaan palo- ja varkausturvalliseen paikkaan talteen.

Jos TrueCryptillä salaa myös niin sanotun järjestelmäosion, eli sen osan kiintolevystä jolla käyttöjärjestelmä sijaitsee, tulee tietokoneeseen TrueCryptin käynnistysvalikko, jossa käyttäjän tulee syöttää salasansa pian sen jälkeen kun tietokoneeseen on kytketty virran. Järjestelmäosion salauksessa kannattaa myös huomioida, että kiintolevysalaus voi hidastaa tietokoneen toimintaa, kun kaikki tietokoneen käyttö vaatii salauksen purkua ja käsittelyä, eikä vain se kun luottamuksellisia asiakirjoja käsitellään. Toisaalta nykyp koneet ovat varsin tehokkaita ja suorituskykyä riittää.



TrueCrypt-säilöjen avaamiseen voi käyttää pelkän salasanan lisäksi myös avaintiedostoja tai älykorttia. Avaintiedostona voi käyttää mitä tahansa käyttäjän valitsemaa tiedostoa.

Salasana on heikoin lenkki

Koska ihmisiä ei yleensä kiinnosta opetella ulkoa monimutkaisia salasanoja, on salasana yleensä salausohjelmistojen heikoin lenkki. Tästä syystä TrueCrypt tukee myös vaihtoehtoisia keinoja, kuten avaintiedoston käyttöä. Mikäli avaintiedosto on käytössä, tulee käyttäjän antaa salasanan lisäksi TrueCryptille polku avaintiedostoon. Avaintiedoston ei tarvitse olla erityisesti salasanakäyttöön tehty, vaan mikä tahansa tiedosto käy, kuten vaikkapa musiikkikappale tai valokuva. Ihmisen keksimä salasana on yleensä alle kahdeksan merkkiä, mutta kolmen megatavun musiikkikappaleen käyttäminen salasanana mahdollistaa huomattavasti pidemmän merkkijonon käyttämisestä salasanana. TrueCrypt tukee myös älykorttien käyttöä salasanan rinnalla tai sijasta.

Vaikka salasanojen käyttöä voi välttää monessa ohjelmassa, kertyy muistettavia salasanoja silti varsin monta. Silloin tarvitaan salasanahygieniaa, jotta salasanat olisivat erilaisia, riittävän monimutkaisia ja turvallisesti säilytettyjä. Onneksi tähänkin tarpeeseen löytyy apuohjelma, jonka esitellään seuraavassa Turvallisuus-lehden numerossa.

Algoritmit ja salaustaso

TrueCrypt tukee lukuisia salausalgoritmejä kuten AES, Serpent ja Twofish. Lisäksi salausavainten pituudet voi valita itse. Jos algoritmien päälle ei ymmärrä, kannattaa käyttää ohjelman ehdottamia oletusasetuksia. Kokonaisturvallisuuden kannalta algoritmeilla ei nykypäivänä ole kuitenkaan suurta merkitystä. Tärkeämpää on mm. salasanahygienia ja varmuuskopioinnin muistaminen!

TrueCrypt sopii Windowsille

TrueCrypt on tällä hetkellä tavalliselle käyttäjälle paras salausohjelma Windowsissa. TrueCryptin voi asentaa myös Maciin tai Linuxiin, mutta näille käyttöjärjestelmille löytyy myös parempia salausohjelmia arkikäyttöön.

Esimerkiksi uusin Ubuntu Linux sisältää ecryptfs-salausjärjestelmän, jolla voi salata jokaisen käyttäjän koko kotihakemiston (Unix-pohjaisissa käyttöjärjestelmissä se sisältää käyttäjän kaikki tiedostot ja myös ohjelmien käyttäjäkohtaiset asetukset). Salaus perustuu käyttäjän sisäänkirjautumissalasanaan, ja kotihakemisto aukeaa ja sulkeutuu automaattisesti kun käyttäjä kirjautuu sisään tai ulos. Näin edes ylläpitäjä ei pysty avaamaan salattua kotihakemistoa, jos käyttäjä ei ole kirjautunut tietokoneeseen.

Murretaan myytti: ”Avoin ohjelma ei ole turvallinen, koska kuka tahansa voi nähdä lähdekoodista miten se toimii.” Murretaan myytti: ”Avoin ohjelma ei ole turvallinen, koska kuka tahansa voi nähdä lähdekoodista miten se toimii.”

Salaus perustuu aina johonkin salaisuuteen. Ainoa turvallinen salausmenetelmä on sellainen, jossa salaisuutena on salasana eikä menetelmän toimintaperiaate. Sillä jos menetelmän toimintaperiaatteeseen perustuva salaus murtuu, vaarantuvat kaikki sillä tekniikalla salatut tiedot, kun taas salasanaan perustuvassa menetelmässä vaarantuvat vain murtuneella avaimella salatut tiedot.

Avoimessa ohjelmassa **ainoa salaisuus on** käyttäjän hallussa oleva **salausavain**. Lähdekoodissa käytettävät menetelmät ovat kaikki julkisia, ja niistä on tehty lukuisia tutkimuksia yliopistoissa ja yrityksissä ympäri maailman. Menetelmään luotetaan vasta, kun näyttää siltä, ettei

kukaan maailmassa keksi siitä heikkoutta vuosikausiin. Suljetut ohjelmat ovat mustia laatikoita, joita akateemikot eivät edes viitsi tutkia. Maailman tunnetuin tietoturva-asiantuntija ja tutkija Bruce Schneier on todennut, että *ohjelman lähdekoodin avoimuus on edellytys tietoturvalle*.

Vain avoimet ohjelmat voivat olla todella turvallisia. Haavoittuvuustietokantojen tilastot tukevat tätä käsitystä: suljetuista ohjelmista paljastuu enemmän ja vakavampia tietoturva-aukkoja ilman, että lähdekoodi on edes luettavissa.

Turvallisuus on aina yhtä vahvaa kuin ketjun heikoin lenkki ja kiitos avoimuuden, heikkoudet on helpompi löytää ja hallita. **Vaikka avoimuus lisää luotettavuutta, ei sekään ratkaise kaikkia ongelmia.** Puolustuksen syvyyttä eli tietoturvaa monella tasolla tarvitaan!

Lähde ja lisenssi

Tämä artikkeli on alun perin julkaistu [Turvallisuus-lehdessä](#) 6/2009.

Copyright Otto Kekäläinen ja Turvallisuus-lehti 2009.

Artikkeli on julkaistu VALO-CD:llä tekijän ja Turvallisuus-lehden toimituksen luvalla.

Artikkelissa mainittu ohjelma on asennettavissa VALO-CD:ltä.