KARELIA-AMMATTIKORKEAKOULU
Tietojenkäsittelyn koulutusohjelma

Vesa Viljanen

YKSITYISYYDEN SUOJAN PARANTAMINEN TIETOVERKOISSA

Opinnäytetyö
Huhtikuu 2013

Karelia AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Huhtikuu 2013
Tietojenkäsittelyn koulutusohjelma

Karjalankatu 3
80200 JOENSUU
p. (013) 260 600

Tekijä

Vesa Viljanen

Nimeke
Yksityisyyden suojan parantaminen tietoverkoissa

Toimeksiantaja
Pohjois-Karjalan ammattikorkeakoulu

Tiivistelmä

Opinnäytetyön aiheena oli tutkia, kuinka tietoverkkojen yksityisyyden suojaa voitaisiin kehittää kotikäyttäjän kannalta. Tarkoituksena oli löytää keinoja, joiden avulla yksityisyyden suojaa voitaisiin helposti edistää ja siten taata turvallinen viestintä. Työssä tutustuttiin alan tietokirjallisuuteen sekä verkkolähteisiin ja löydettyjä ohjelmistopohjaisia ratkaisuja yksityisyyden suojan edistämiseksi testattiin empiirisesti itse.

Tutkimuksessa ilmeni, että lainsäädännön tarjoama turva ei ole riittävä ja että käyttäjältä vaaditaan omaa panostusta, mikäli viestintä halutaan suojata. Jotta verkkorikoksia ja laajalti levinneitä haittaohjelmia voidaan estää, on tietoturvataso rakennettava kunnolliseksi ja sitä on ylläpidettävä jatkuvasti. Verkkomainonta ja tiedonlouhinta ovat yleistyneet räjähdysmäisesti, mikä asettaa uudet normit oman yksityisyyden varjelemiselle. Sosiaalinen media tuo oman näkökulmansa yksityisyyden suojan kysymykseen pakottamalla käyttäjät kyseenalaisiin tietosuojaehtoihin.

Tulokset osoittivat, että kotikäyttäjän on syytä hyödyntää erilaisten verkkoprotokollien ja niitä hyödyntävien ohjelmien, palveluiden ja tekniikoiden tarjoamaa suojaa. Työssä on esitelty erilaisia vaihtoehtoisia toimintamalleja ja sovellusehdotuksia, joita on mahdollista hyödyntää yksityisyyden takaamiseksi. Pääpaino esitetyissä ratkaisuissa oli ilmaisissa ja avoimeen lähdekoodiin perustuvissa ohjelmissa ja palveluissa. Tutkimus julkaistiin myös Internetissä osoitteessa http://www.yksityisyydensuoja.fi.

Kieli
suomi

Sivuja 85

Asiasanat
yksityisyys, tietosuoja, tietoturva, anonymiteetti

THESIS
April 2013
Degree Programme in
Business Information Technology

Karjalankatu 3
80200 JOENSUU, FINLAND
Tel. +358 13 260 600

Author

Vesa Viljanen

Title
Enhancing Privacy Protection in Information Networks

Commissioned by
North Karelia University of Applied Sciences

Abstract

The aim of this study was to investigate how privacy could be improved in information networks in relation to the home user. The purpose was to find out ways in which confidentiality could easily be endorsed and how a secure communication could be assured. The theoretical part of the study was based on published literature and online sources concerning privacy and anonymity in computer networks. The research was carried out by testing the presented software-based solutions empirically.

The study revealed that the security provided by the law is not adequate enough, and the user is required to take supplementary actions to protect the network communications properly. In order to prevent cybercrimes and widely spread malicious software, the user has to uphold a decent level of security with constant maintenance. Online advertising and data mining have increased exponentially, and these set new standards for the privacy protection. Additionally, social media brings its own aspect by prompting users to accept questionable privacy policies. Therefore, a lot of knowledge and expertise in numerous programs and techniques is required.

The results showed that the user should take advantage of a variety of network protocols, programs, services and technologies that increase protection. The topics of the thesis represented and discovered alternative approaches and suggested several applications which can be utilized to guarantee the privacy and security of a home user. The main focus in the presented solutions was placed on free services and open source software. The study is also available on the Internet at http://www.yksityisyydensuoja.fi.

Language
Finnish

Pages 85

Keywords
privacy, confidentiality, information security, anonymity

Sisällys

Kuva- ja kuvioluettelo

1 Johdanto

Tänä päivänä tietoverkkojen käyttäjiä tarkkaillaan laajamittaisesti eri organisaatioiden toimesta, yksityisyyden suojaa vähätellään ja tietosuojaehdoilla poljetaan käyttäjien oikeuksia. Internetissä asioimisesta tallentuu tietoja eri palvelimille ilman, että käyttäjällä on mahdollisuutta siihen itse vaikuttaa. Alalle onkin syntynyt suuri bisnes, jossa tieto on arvokasta.

Tämän tutkielman tarkoituksena on selvittää, kuinka kotikäyttäjien yksityisyyden suojaa tietoverkoissa voitaisiin parantaa. Opinnäytetyön toimeksiantaja on Pohjois-Karjalan ammattikorkeakoulun tietojenkäsittelyn koulutusohjelma, ja työn tavoitteena on tutkia sekä löytää erilaisia keinoja turvalliseen ja suojattuun viestintään. Tutkimuksessa tarkastellaan tietoverkkojen käyttämiseen liittyviä aihealueita yksityisyyden suojan näkökulmasta. Näitä ovat mm. hyvän tietoturvatason ylläpitäminen, luotettava tietojenkäsittely, anonyymi ja turvallinen www-sivujen selaaminen, suojattu tiedonsiirto, pikaviestinnän ja sähköpostiviestien salaaminen sekä anonyymien tietoverkkojen käyttäminen. Aihealue rajataan koskemaan lähinnä henkilökohtaisia tietokoneita (*personal computer*), mutta käytännössä samat menetelmät, protokollat ja osa mainituista sovelluksista toimivat myös monissa muissa laitteissa. Tutkimuksesta jätetään pois myös VoIP-protokolla (*voice over internet protocol*), jolla tarkoitetaan teknologiaa äänen reaaliaikaiseen siirtoon verkon välityksellä. Rajaus tehdään sen vuoksi, että VoIP:ta tukevia tehokkaita salaustekniikoita ja ohjelmistoja ei ole vielä testattu laajamittaisesti, eikä niiden voida siksi olettaa tarjoavan luotettavaa suojaa.

Tutkielmassa käsitellään ensin perusteet työn aihepiiristä kuvaamalla nykyisen lainsäädännön puitteet, yksityisyyden suojan merkitys kotikäyttäjän kannalta sekä tiedon ympärillä liikkuva bisnes. Teoreettisen osuuden jälkeen selostetaan teknistä puolta ja aiheiden yhteydessä kerrotaan keinoista, joilla yksityisyyden suojaa voidaan parantaa. Ensin liikutaan perustavanlaatuisissa tietoturvallisuuden kysymyksissä, minkä jälkeen siirrytään kuvaamaan tutkielman kannalta tärkeitä verkkoprotokollia ja anonyymejä verkkoja. Viimeisenä laajana

kokonaisuutena työstetään suojattua viestintää. Lopuksi kokonaisuudesta koostetaan yhteenveto, joka tiivistää tutkimuksessa löydetyt merkittävimmät keinot yksityisyyden suojan parantamisen kannalta.

2 Yksityisyyden suoja

Yksityisyyden suojalla tarkoitetaan tässä tutkielmassa luonnollisen henkilön oikeutta ja käytännön mahdollisuutta suojautua ulkopuoliselta tarkkailulta tietoverkoissa. Sillä tarkoitetaan esimerkiksi Internetin kautta saatavissa olevien henkilökohtaisten tietojen suojaamista. Näitä ovat mm. henkilötiedot, paikannustiedot, viestintätiedot ja teletunnistetiedot. Kun käyttäjän yksityisyyden suoja ei ole riittävä, on myös hänen sananvapautensa uhattuna. Jokaisella kansalaisella on oikeus määrätä omien henkilötietojensa käytöstä ja niiden jakamisesta. Sanastokeskus (2004, 11) määrittelee yksityisyyden suojan käsitteen seuraavalla tavalla:

Oikeus yksityisyyteen, johon kuuluu muun muassa oikeus määrätä itseään koskevista asioista ja tiedoista sekä oikeus kotirauhaan ja luottamukselliseen viestintään, vrt. *luottamuksellisuus*. Esimerkiksi oikeudeton henkilötietojen käsittely tai kameravalvonta tai roskapostin lähettäminen sähköpostitse voi loukata henkilön yksityisyyden suojaa.

Käsite sekaantuu kuitenkin helposti *tietosuoja*-termiin. Tietosuojalla tarkoitetaan ihmisen yksityisyyden suojaa ja muita sitä turvaavia oikeuksia henkilötietoja käsiteltäessä. Näitä ovat muun muassa tietojen valtuudettoman saannin estäminen ja tietojen luottamuksellisuuden säilyttäminen sekä henkilötietojen suojaaminen valtuudettomalta tai henkilöä vahingoittavalta käytöltä. (Valtiovarainministeriö 2008, 105.) Vaikka termit ovat hyvin lähellä toisiaan, tämän tutkielman tarkoitusperiä kuvaa paremmin termi *yksityisyyden suoja*, koska tietosuoja on näin katsottuna yksityisyyden suojan osa-alue.

2.1 Lainsäädäntö

Oikeus yksityisyyden suojaan on Suomen perustuslain turvaama henkilöllinen oikeushyvä eli oikeusjärjestyksen suojelema etu. Suomen perustuslain (731/1999) 10 §:n mukaan henkilötietojen suojasta säädetään lailla. Henkilötietojen käsittelyä koskevia erillisiä vaatimuksia tulee osaltaan myös Euroopan unionin normeista sekä muista kansainvälisistä säännöksistä, normeista ja suosituksista. Yksityisyyden suojaan vaikuttavat lait ovat henkilötietolaki (523/1999), laki viranomaisten toiminnan julkisuudesta (621/1999), laki yksityisyyden suojasta työelämässä (759/2004), sähköisen viestinnän tietosuojalaki (516/2004) sekä EU:n direktiivit: henkilötietodirektiivi (46/1995/EY) ja sähköisen viestinnän tietosuojadirektiivi (58/2002/EY).

Sähköisen viestinnän tietosuojalaki on suomalaisittain merkittävin laki tietoverkoissa toimiessa. ”Lain tarkoituksena on turvata sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan toteutuminen sekä edistää sähköisen viestinnän tietoturvaa ja monipuolisten sähköisen viestinnän palvelujen tasapainoista kehittymistä” (516/2004). Kyseisen lain 4 §:n mukaan verkkosivujen selaamisesta kertyvät tunnistamistiedot ovat luottamuksellisia, jollei niistä erikseen toisin säädetä. Sähköisen viestinnän tietosuojalakiin lisättiin merkittävä muutos toukokuussa 2008 (343/2008), jolloin säädettiin teletunnistamistietojen tallentamisesta. Kyseinen muutos oli seurausta EU:n direktiivistä (24/2006/EY), jolla teleyritykset velvoitettiin säilyttämään kaikkien viestintää harjoittavien tilaajien ja käyttäjien tunnistamistiedot sekä tietyt muut tiedot. Direktiivin mukaan tiedot on säilytettävä vähintään kuuden kuukauden ajan ja enintään kahden vuoden ajan. Poliisilla on lain mukaan oikeus saada teletunnistetietoja teleyritykseltä tiettyjen vähäisten viestintään liittyvien rikosten selvittämiseksi. Suomessa sähköisen viestinnän tietosuojalain (516/2004) 14 §:n mukaan teleyritysten tulee säilyttää tunnistetiedot viranomaistarpeita varten 12 kuukauden ajan viestinnän päivämäärästä. Perustuslaissa (731/1999) määritellään poliisin oikeuksista tunnistetietojen suhteen seuraavasti:

Viranomaisten oikeudesta saada tunnistamistietoja rikosten ennalta estämiseksi ja paljastamiseksi säädetään poliisilaissa (493/1995) ja tullilaissa (1466/1994).

Viranomaisten oikeudesta saada tunnistamistietoja rikoksen selvittämiseksi säädetään pakkokeinolaissa (450/1987).

Suomen ja EU:n lakien tarjoama suoja yksityisyydelle ei kuitenkaan ole riittävä. Esimerkiksi Ruotsin puolustusministeriön alainen organisaatio Försvarets radioanstalt eli FRA saa seurata ja salakuunnella kaikkea Ruotsin läpi kulkevaa viestiliikennettä. Ruotsin parlamentti hyväksyi 18.6.2008 niin sanotun FRA-lain eli Ruotsin viestintätiedustelulain (2008:717), joka astui voimaan 1.1.2009. Lain turvin FRA pystyy valvomaan kaikkea Ruotsiin kulkevaa nettiliikennettä. Laki koskee suurelta osin myös suomalaisia, koska merkittävä osa ulkomaille suuntautuvasta Internet-liikenteestä kulkee Ruotsin kautta.

Verkkopalveluissa yksityisyyden suojaan vaikuttaa usein sen maan laki, jossa palvelu toimii. Esimerkiksi useat suositut verkkopalvelut toimivat Yhdysvalloissa, ja tällöin yksityisyyden suojaa ajatellen niitä velvoittaa muun muassa USA PATRIOT -laki (Pub. L. No. 107–56, 2001). Kyseinen laki antaa esimerkiksi FBI:lle mahdollisuuden pakottaa Yhdysvalloissa toimivien verkkopalveluiden tarjoajat luovuttamaan asiakastietojaan kansallisen turvallisuusuhan nimissä. Tämä voidaan tehdä kaiken lisäksi ilman käyttäjien tietoisuutta ja ilman normaalia, pitkäkestoisempaa oikeusmenettelyä.

Yhdysvalloissa verkkopalveluita velvoittaa myös ulkomaisten kansalaisten vakoilulaki vuoden 2008 lainmuutoksineen. Tämän FISAA-lain nimi tulee sanoista Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (Pub. L. No. 110–261). Laki antaa viranomaisille oikeuden tarkkailla kaikkia ulkomaisten henkilöiden kanssa yhteydessä olevia. Sen mukaan USA:n hallinto voi vakoilla sähköposteja ja puheluita, jotka tulevat Yhdysvaltoihin tai lähtevät sieltä. Laki koskee myös USA:ssa toimivia pilvi- ja sähköpostipalveluita, joiden yksityisyyden suojaa ei voida tämän takia taata. Tammikuussa 2013 kyseinen FISAA-lainsäädäntö vahvistettiin, ja Yhdysvallat antoi viiden vuoden lisäajan lain lisäyksille, jotka antavat USA:n viranomaisille oikeuden seurata maasta lähtevää ja maahan tulevaa puhelinliikennettä sekä sähköistä tiedonkulkua ilman rajoituksia (RT 2013).

Edellä mainitut Yhdysvaltojen terrorismin vastaisen sodan perusteella luodut lait vaikuttavat huomattavissa määrin EU:n kansalaisten oikeuksiin ja yksityisyyden suojaan. FISAA mahdollistaa EU:n kansalaisten ja organisaatioiden reaaliaikaisen viestiliikenteen ja pilvipalveluihin tallennetun tiedon tarkkailun ilman rikosepäilyä. Lain turvin Yhdysvallat voi esimerkiksi tarkkailla eurooppalaisia poliitikkoja, aktivisteja ja toimittajia vedoten Yhdysvalloille poliittisesti tärkeisiin aiheisiin. On hyvä myös tiedostaa, että mm. Microsoftin, Googlen ja Amazonin kaltaisten organisaatioiden verkkopalveluihin tallennettu tieto on samoihin lakeihin vedoten tietosuojaltaan epäluotettavaa. Yksityisyyden suojaa yritetään myös aktiivisesti kaventaa uusilla lakiehdotuksilla. Tästä esimerkkeinä ovat viime vuosina ehdotetut lakimuutokset, joita ovat seuraavat: ACTA (*Anti-Counterfeiting Trade Agreement*), SOPA (*Stop Online Piracy Act*), PIPA (*Protect Real Online Threats to Economic Creativity and Theft of Intellectual Property Act*) ja CISPA (*Cyper Intelligence Sharing and Protection Act*). Ehdotusten perusteella voidaan olettaa, että paine yksityisyyden suojan leikkaamiselle lisääntyy ja tulevaisuudessa uudet lakimuutokset tulevat todennäköisemmin kaventamaan käyttäjien yksityisyyden suojaa entisestään.

2.2 Yksityisyyden suojan merkitys

Yksityisyyden suojan arvostus on kokenut 2000-luvulla varsinaisen inflaation. Sosiaalinen media on tullut jäädäkseen, ja käyttäjät ovat uusien palveluiden myötä yhä valmiimpia luopumaan yksityisyydestään. Suositun verkkoyhteisöpalvelu Facebookin aktiivisten käyttäjien määrä ylitti miljardin rajan syyskuun puolivälissä 2012 (Zuckerberg 2012). Facebookiin liittyessään käyttäjä tarjoaa henkilökohtaista tietoa itsestään ja usein kutsuu vielä ystävänsä ja perheensä palvelun pariin, mikäli heillä ei ole omaa tiliä. Tämän jälkeen palveluun jaetaan monenlaista lisätietoa, kuten pidettyjä ja vihattuja asioita, omia mielipiteitä ja valokuvia. Yhteydenpito ystävien kanssa hoituu helposti, mutta kääntöpuolena kaikki tieto tallentuu Facebookin palvelimille ja on pahimmassa tapauksessa haluamattakin kaikkien saatavilla. Sosiaalisen median tarjoamat tietomäärät ovat kuin kultakaivos erilaisille organisaatioille. Käyttäjien käyttäytymistä ja terveysriskejä voidaan seurata, poliittista vakaumusta voidaan

hyödyntää kampanjoissa, mainokset voidaan kohdentaa mahdollisimman tehokkaasti ja tarkasti sekä terrorismista tai muusta rikollisesta toiminnasta epäiltyjä voidaan tarkkailla paremmin. Tähän kaikkeen käyttäjä itse antaa suostumuksensa. Facebookin tietosuojaehdoissa (Facebook 2012) kuvataan tietojen keräämistä seuraavalla tavalla:

> Saamme tietoa aina, kun olet yhteydessä Facebookiin, esimerkiksi kun katsot toisen käyttäjän aikajanaa, lähetät jollekulle viestin tai saat viestin, etsit kaveria tai sivua, klikkaat tai tarkastelet jotain asiaa tai olet muuten yhteydessä siihen, käytät Facebook-mobiilisovellusta, ostat Facebook-krediittejä tai teet muita ostoksia Facebookin kautta.
>
> Kun julkaiset Facebookissa esimerkiksi kuvia tai videoita, saatamme saada muuta julkaisuun liittyvää tietoa (metatietoa), kuten kellonajan, päivämäärän ja tiedon paikasta, jossa otit kuvan tai kuvasit videon.
>
> Saamme tietoja tietokoneesta, matkapuhelimesta tai muusta laitteesta, jolla käytät Facebookia, mukaan lukien sen, kun useat käyttäjät kirjautuvat sisään samasta laitteesta. Tällaisia tietoja saattavat olla IP-osoitteesi, käyttämäsi Internet-palveluntarjoaja, sijaintisi, käyttämäsi selain (mukaan lukien selaimen tunnisteet) tai sivut, joilla vierailet. Saatamme esimerkiksi saada GPS-sijaintisi tai muita sijaintiasi koskevia tietoja, jotta voimme kertoa, onko joku kavereistasi lähellä.
>
> Saamme tietoja aina, kun käytät peliä, sovellusta tai sivustoa, joka käyttää Facebook-sovellusalustaa, tai käyt sivustossa, jossa on Facebook-toiminto (esim. yhteisöliitännäinen), joskus evästeiden avulla. Tällaisia tietoja saattavat olla vierailusi päivä ja aika, sivusto eli URL-osoite, jossa olet, teknisiä tietoja käyttämästäsi IP-osoitteesta, selaimesta ja käyttöjärjestelmästä ja käyttäjätunnuksesi, jos olet kirjautuneena Facebookiin.
>
> Joskus saamme tietoja mainoskumppaneiltamme, asiakkailta ja muilta kolmansilta osapuolilta, jotka auttavat meitä (tai heitä) toimittamaan mainoksia, analysoimaan toimintaa verkossa ja yleisesti parantamaan Facebookia. Mainostaja saattaa esimerkiksi kertoa meille tietoja sinusta (esim. miten reagoit mainokseen Facebookissa tai toisessa sivustossa) tarkoituksena mitata mainosten tehokkuutta ja parantaa niiden laatua. Yhdistämme myös tietoja, joita meillä jo on sinusta ja kavereistasi. (Facebook 2012.)

Facebook on vain yksi monista yrityksistä, jotka käyttävät suuria tietokantojaan hyödyksi seulomalla myös käyttäjien yksityisiä keskusteluja ja henkilökohtaista materiaalia. Maaliskuussa 2012 Facebookin automaattiset haut löysivät Floridasta epäilyttävää toimintaa reilun 30-vuotiaan miehen ja 13-vuotiaan tytön väliltä, minkä jälkeen yrityksen työntekijät raportoivat pedofiliaepäilystä poliisille

(Menn 2012). Vaikka tällainen toiminta on varmasti hyödyllistä rikosten estämiseksi, herättää se kuitenkin paljon kysymyksiä käyttäjien yksityisyyden suojasta. Vastaavia julkisesti raportoituja tapauksia ei ole useita Internetissä toimivien organisaatioiden joukossa. Tämä voisi viitata siihen, että konkreettiset tulokset rikosten estämiseksi jäävät kohtuullisen pieniksi. Toiseksi ammattimaiset rikolliset käyttävät huomattavasti suojatumpia keinoja verkoissa toimimiseen, minkä vuoksi tämän kaltaisen seurannan avulla saadaan käytännössä kiinni vain vähäpätöisempiä tekijöitä. Yksityisyyden suojaa tällainen toiminta sen sijaan heikentää merkittävästi, koska seurannan kohteeksi joutuvat kaikki palveluiden käyttäjät.

Usein ajatellaan, että yksityisyyden loukkaukset koskevat vain rikollisia. Lisäksi tavalliset käyttäjät ovat taipuvaisia olettamaan, ettei mahdollisesta tarkkailusta ole varsinaista haittaa, koska omia tietoja ei koeta salaamisen arvoisiksi. Tietoturvayhtiö F-Securen tutkimusjohtaja Mikko Hyppönen (2011) selvitti TED-konferenssissa pitämässä puheessaan, ettei yksityisyyden suojan kysymyksessä valita yksityisyyden ja turvallisuuden välillä, vaan vapauden ja valvonnan välillä. Puheessaan hän painotti sitä, että kun annamme muille valtuuksia yksityisyyden suojaamme koskien, hyväksymämme valtuudet tulevat usein jäädäkseen. Esimerkiksi jos hyväksymme sen, että valtiot saavat tarkkailla kansalaisiaan asentamalla takaportteja avaavia haittaohjelmia kansalaisten koneelle, käytännöstä tulee lopulta pysyvä ja yleisempi. Puheessaan Hyppönen (2011) viittasi muun muassa Saksan poliisivoimien käyttämään Bundestrojaner-haittaohjelmaan, jolla Saksan valtio on tarkkaillut omia kansalaisiaan. (Hyppönen 2011.)

Bundestrojaner-haittaohjelma ei pelkästään lähetä saastuneen tietokoneen tietoja hyökkääjille, vaan se tarjoaa etäyhteyden kautta myös mahdollisuuden tiedostojen lähettämiseen ja suorittamiseen saastutetulla koneella. Tämän lisäksi troijalaisen merkittävät suunnitteluvirheet tarjoavat saman tilaisuuden haittaohjelman käyttämiseen muillekin kuin vain Saksan poliisille. (Chaos Computer Club 2011.) Näin ollen Saksan kansalaiset joutuivat oman valtion toimien vuoksi vakavaan tietoturvauhkaan. Troijalaisen luonut DigiTask-yhtiön puhemies Winfried Seibert on kertonut, että yritys on myynyt samankaltaisia

haittaohjelmia myös Itävallan, Sveitsin ja Hollannin hallituksille (Farivar 2011). Kuten Bundestrojaner-haittaohjelman tapaus osoittaa, kyseenalaista valtiollista tarkkailua on harrastettu jo pitkään useissa eri maissa. Tämän vuoksi eurooppalaistenkin on hyvä huomioida mahdollinen uhka yksityisyyden suojalleen.

Seuraavaksi kerrotaan muita esimerkkejä valtion tarkkailusta maailmalta: Ihmisoikeusryhmät ovat raportoineet useista eri tapauksista, joissa Iranin hallitus valvoo kansalaistensa puheluita ja verkkoliikennettä. Kiinalainen ZTE Corp -organisaatio on viime vuosien aikana myynyt ja toimittanut 98,6 miljoonan euron edestä verkkoliikennelaitteita hallituksen kontrolloimalle teleyhtiölle, jolla on lähes monopoliasema Iranin lankapuhelinverkosta. Tämän lisäksi suurin osa Iranin Internet-liikenteestä kulkee organisaation kautta. Entinen Iranin tietoliikenteen projektipäällikkö Mahmoud Tadjallimehr kertoo, että maan hallitus pystyy nykyisin paikallistamaan nopeasti teleliikenteen käyttäjät. Tämän lisäksi puhelinliikenne, tekstiviestit, sähköpostit, chat-keskustelut ja Internetiin pääsy voidaan siepata ja tarvittaessa estää. (Stecklow 2012.) Kiinassa on puolestaan ollut jo vuosia käytössä suuri palomuuri (*Golden Shield*), joka sensuroi ja tarkkailee kansalaisten verkkoliikennettä. Googlen puhemies Eric Schmidtin mukaan Kiinan hallitus on ainoa valtioneuvosto, joka käyttää aktiivista ja dynaamista sensuuria sekä kybervakoilua kansalaisiaan kohtaan (Rogin 2012).

Tiedustelupalvelut ja eri maiden keskusrikospoliisit ovat olleet jatkuvasti kiinnostuneita omien oikeuksiensa lisäämisestä ja kansalaisten yksityisyyden suojan kaventamisesta. McCullagh (2012) kirjoittaa, että viime vuosina Yhdysvaltain liittotutkimusvirasto FBI on yrittänyt Going Dark -projektillaan saada useita suuria Internet-yhtiöitä ja verkkopalveluita sisällyttämään takaovia omiin ohjelmiinsa valtiollista tarkkailua varten. Projektiin halutaan mukaan mm. Microsoft, Facebook, Yahoo ja Google tuotteineen. Mikäli FBI saa tahtonsa läpi, se voi tarkkailla kansalliseen turvallisuuteen vedoten kenen tahansa tietoja projektissa mukana olevien organisaatioiden avulla. (McCullagh 2012.)

Tiedustelupalveluiden kansainvälisestä tarkkailusta on todisteena myös Echelon-viestintäsieppausjärjestelmä, jonka toimintaan osallistuvat yhteistyössä

Yhdysvallat, Yhdistynyt kuningaskunta, Kanada, Australia ja Uusi-Seelanti. Järjestelmä perustuu erityisesti satelliittiviestinnän maailmanlaajuiseen sieppaukseen ja sen tarkoituksena on yksityisen ja kaupallisen viestinnän sieppaaminen. (EYVL 2002, 222.) Euroopan parlamentin päätöslauselmassa (EYVL 2002) otetaan huomioon myös muiden sieppausjärjestelmien mahdollisuus, ja niistä kerrotaan seuraavasti:

> Muiden sieppausjärjestelmien olemassaolon mahdollisuus ottaa huomioon, että viestinnän sieppaaminen on tiedustelupalvelujen yleisesti käyttämä vakoilukeino ja myös muut valtiot voisivat pitää yllä vastaavanlaista järjestelmää, jos niillä on siihen riittävät taloudelliset ja maantieteelliset mahdollisuudet; katsoo Ranskan olevan ainoa EU:n jäsenvaltio, joka merentakaisten alueidensa ansiosta pystyisi maantieteellisesti ja teknisesti käyttämään itsenäisesti maailmanlaajuista sieppausjärjestelmää, ja lisäksi sillä on tähän tarvittava tekninen ja organisatorinen infrastruktuuri; ottaa myös huomioon runsaat todisteet siitä, että Venäjä todennäköisesti pitää yllä vastaavaa järjestelmää. (EYVL 2002, 223.)

Ristiriitaa EU:n oikeuden kanssa ei synny, mikäli viestintäsieppausjärjestelmää käytetään vain tiedustelupalvelutarkoituksiin. Tämä johtuu siitä, että valtion turvallisuutta palvelevat toiminnot eivät kuulu Euroopan yhteisön perustamissopimuksen soveltamisalaan. Euroopan ihmisoikeussopimuksen yksityisyyttä suojaava 8 artikla sallii, että yksityisyyteen voidaan puuttua ainoastaan kansallisen turvallisuuden takaamiseksi. Tämä edellyttää sitä, että säännökset on kirjattu kansalliseen lainsäädäntöön ja ne ovat yleisesti saatavilla. Lisäksi niissä on säädettävä, missä oloissa ja millä ehdoilla valtiovalta saa kyseisiä toimia toteuttaa. (EYVL 2002, 223.) Näillä perusteilla tiedustelupalveluiden on laillista vakoilla kansalaisia Echelon-järjestelmän avulla. Euroopan parlamentin päätöslauselmassa kehotetaankin kaikkia kansalaisia salaamaan sähköpostiviestit, jotka ovat salaamattomana ulkopuolisten kaapattavissa (EYVL 2002, 225).

Edellä olevien seikkojen perusteella voidaan olettaa, että yksityisyyden suojan kaventaminen kansalliseen ja kansainväliseen turvallisuuteen vedoten tulee lisääntymään tulevaisuudessa valtioiden taholta. Lisäksi kaupalliset organisaatiot ovat yhä kiinnostuneempia hyödyntämään ja myymään keräämiään käyttäjätietoja. Vaikka useat Internetin palvelut on tehty houkutteleviksi mm.

ilmaisuuden ansiosta, niihin liittyvät riskit on kuitenkin hyvä huomioida jo ennen palveluiden käyttöönottoa.

2.3 Tietoa hyödyntävät osapuolet

Nykypäivänä annamme informaatiota itsestämme muille enemmän kuin mikään ryhmä aiemmin ihmiskunnan historiassa. Tätä tietoa myös kerätään ja yhdistellään enemmän kuin koskaan ennen. Suurimman osan annamme pois helppokäyttöisyyden ja ilmaisten tai lähes ilmaisten palveluiden käytön takia. Vaihdamme henkilökohtaiset tietomme mukavuuksiin, kuten verkkokauppojen käyttöön, pikaviestimiin ja sosiaalisen median sovelluksiin. Nämä tiedot kuitenkin yhdistellään ja luokitellaan monin eri tavoin: sukupuolen, iän, tulotason, asuinpaikan, mielipiteiden, kiinnostusten kohteiden ja sivuhistorian suhteen. Käyttäjät ryhmitellään käyttäytymisen mukaan, ja luokitellut ryhmät vuokrataan tai myydään eteenpäin mainostajille, jotka käyttävät tietoja hyväkseen omissa kampanjoissaan. (Craig & Ludloff 2011, 1–2.) Kaikki tämä tietoverkoista tallennettu informaatio on arvokas kaupankäynnin kohde, ja tämän vuoksi peliin osallistuvat monet erilaiset organisaatiot. Näitä valtavia tietomääriä käyttävät osapuolet voidaan luokitella neljään laajaan ryhmään: tiedon kerääjät, tiedon louhijat, tiedon käyttäjät ja tiedon seuraajat (Craig & Ludloff 2011, 45).

Tiedon kerääjillä tarkoitetaan henkilöitä, jotka keräävät erillisistä lähteistä tallennetun informaation, kuten esimerkiksi matkapuhelimista, kauppojen kanta-asiakaskorteista, valvontakameroista ja RFID-tunnisteista (*Radio Frequency Identification*) saadut tiedot. Käyttäjät antavat tietoa edellä mainituille lähteille yleensä vapaaehtoisesti, mutta usein myös tiedostamattaan. Normaalisti tiedot hyödynnetään joko markkinointitarkoituksiin tai myydään kolmansille osapuolille (Craig & Ludloff 2011, 45).

Tiedon louhijat koostavat informaatiota henkilötietoja sisältävistä tietopankeista ja myyvät tietoja eteenpäin. Kerätyt lähdetiedot saattavat koostua esimerkiksi julkisista tai kaupallisista tietokannoista sekä rikosrekistereistä. Lopuksi louhittu tieto pakataan ja raportoidaan koostetiedoiksi, minkä jälkeen nämä myydään

yrityksille ja organisaatioille sekä tiedustelupalveluille. Tietoja ostetaan varsinkin työntekijöiden taustaselvityksiä varten, mutta saatu tieto on hyödyllistä myös markkinointitarkoituksissa. Tiedon louhintaan erikoistuneita yrityksiä ovat esimerkiksi Acxiom ja ChoicePoint. (Pierce & Ackerman 2005, 3.) Acxiomia on leikkisästi kuvailtu yhdeksi suurimmista yrityksistä, joista kukaan ei ole koskaan kuullutkaan. Yrityksen johtajat ovat kertoneet tietokantojensa sisältävän 500 miljoonan kuluttajan tietoja ympäri maailman. Lisäksi jokaisesta kuluttajasta löytyy noin 1500 erillistä informaatiota. (Singer 2012.)

Tiedon käyttäjät ostavat tietoa tai pääsevät siihen käsiksi ilmaiseksi (Craig & Ludloff 2011, 45). Tiedon käyttäjiksi voidaan luokitella myös henkilöt, jotka hakevat tietoja esimerkiksi Fonectan tarjoamista palveluista. Tiedon seuraajilla tai suojelijoilla puolestaan tarkoitetaan virastoja ja organisaatioita, jotka valvovat yksityisyyden suojan kysymyksiä erilaisista näkökulmista ja ovat mukana säätelemässä menettelytapoja ja ohjeistuksia eri toimialoille ja toiminnoille (Craig & Ludloff 2011, 45). Näitä ovat Suomessa esimerkiksi tietosuojavaltuutettu ja Electronic Frontier Finland ry.

3 Tietoturva

Tietoturvallisuudella pyritään varmistamaan mm. tiedon käytettävyys, eheys ja luottamuksellisuus (Valtionvarainministeriö 2008, 109). Tietoturvan eri osille on omat tekniset ratkaisunsa, mutta tutkielmassa keskitytään erityisesti niihin osa-alueisiin, jotka ovat merkittävimpiä yksityishenkilön yksityisyyden suojalle tietoverkkoja käytettäessä. Seuraavissa alaluvuissa käsitellään virustorjunnan ja palomuurien merkitystä, verkkoselainten ja selainlaajennusten hyödyntämistä yksityisyyden suojaamisessa, tehokkaiden salasanojen käyttöä, salausmenetelmien mahdollisuuksia tiedon turvaamisessa sekä tietojen lopullista tuhoamista.

3.1 Virustorjunta ja palomuuri

Virustorjuntaohjelmistojen tarkoituksena on suojella tietokonelaitteita haittaohjelmilta, joihin kuuluvat mm. loogiset pommit, troijalaiset, takaovet, tietokonemadot, tietokonevirukset, vakoiluohjelmat sekä mainosohjelmat. Loogiset pommit (engl. *logical bomb*) koostuvat kahdesta osasta: tietosisällöstä, joka sisältää suoritettavan toiminteen, sekä kytkimestä, joka laukaisee tietosisällön, kun jokin ennalta määrätty ehto täytyy. Troijalainen (engl. *trojan*, *trojan horse*) puolestaan tarkoittaa viattomaksi naamioitua ohjelmaa, joka kuitenkin suorittaa taustalla vahingollisia toimenpiteitä. Takaovi (engl. *back door*) on mekanismi, joka ohittaa normaalit turvallisuustarkistukset ja päästää ulkopuolisen tahon sisälle järjestelmään. Tietokonevirukset (engl. *virus*) ovat haittaohjelmia, jotka suoritettaessa yrittävät monistaa itseään ja levittäytyä muihin tiedostoihin. Tietokonemadot (engl. *worm*) monistavat myös itseään, mutta ne eroavat tietokoneviruksista kahdella tavalla: ensinnäkin tietokonemadot ovat itsenäisiä haittaohjelmia, jotka eivät ole riippuvaisia muista tiedostoista, ja toiseksi ne leviävät tietoverkkojen avulla tietokoneesta toiseen. Vakoiluohjelmat (engl. *spyware*) ovat ohjelmia, jotka keräävät tietoja tietokoneesta ja lähettävät niitä hyökkääjälle. Mainosohjelmat (engl. *adware*) keräävät myös tietoja käyttäjästä, mutta käyttävät niitä mainostarkoituksiin. (Aycock 2006, 12–17.)

Työasemakäyttöön tarkoitetuilla virustorjuntaohjelmistoilla on kaksi perustilaa: staattinen tiedostojen tarkastustila sekä dynaaminen reaaliaikainen tila. Reaaliaikaisessa tilassa ohjelmisto tarkistaa uudet tiedostot ennen kuin käyttäjä avaa ne ja ehkäisee siten muiden tiedostojen saastumisen. Staattisessa tilassa käyttäjä voi puolestaan suorittaa mm. koko kovalevyn tai muistitikun tarkistuksen. Kuukausittain ilmestyy jopa satoja uusia haittaohjelmia, ja siksi virustorjuntaohjelmiston virustietokantojen säännöllinen päivittäminen on tärkeää. (Viestintävirasto 2007b.)

F-Securen tutkimusjohtaja Mikko Hyppönen (2012) paljasti, että viime vuosien kuuluisimmat haittaohjelmat Flame, Stuxnet ja DuQu toimivat pitkään ennen kuin tietoturvayhtiöt saivat niistä vihiä. Tietoturvayhtiöt eivät tunnistaneet Flamea ainakaan kahteen vuoteen sen ilmestymisen jälkeen. Tuona aikana se sai tarttua

ja toimia rauhassa. Stuxnet ja DuQu puolestaan olivat aktiivisia yli vuoden, kunnes ne tulivat yleiseen tietoon. Kyseiset haittaohjelmat ovat länsimaalaisten tiedustelupalveluiden kehittämiä ja niitä käytettiin pääasiassa poliittisesti kriittisillä alueilla Iranissa, Syyriassa ja Sudanissa. Vaikka haittaohjelmat olisivat kohdennettuja, ne voivat kuitenkin riistäytyä käsistä ja aiheuttaa vahinkoa valittujen uhriensa lisäksi muillekin. Esimerkiksi Stuxnet-tietokonemato levisi ympäri maailmaa ja saastutti yli 100 000 tietokonetta etsiessään todellista kohdettaan, Iranin Natanzin uraanin rikastuslaitosta. Totuus on, että kuluttajaluokan virusturvaohjelmistot eivät tarjoa riittävää suojaa massiivisilla resursseilla toteutettuja, kohdennettuja haittaohjelmia vastaan. Ne suojelevat käyttäjiä vain tyypillisiltä haittaohjelmilta, kuten esimerkiksi pankkitroijalaisilta, näppäilyntallentajilta ja sähköpostimadoilta. (Hyppönen 2012.)

Palomuuri on järjestelmä, joka toteutetaan joko ohjelmisto- tai laitteistopohjaisesti. Se valvoo verkkojen välillä kulkevaa tietoliikennettä ja suojaa tietokonetta ulkopuolelta tulevilta hyökkäyksiltä. Perusedellytyksenä on, että kaikki verkkoliikenne kulkee palomuurin läpi ja että ainoastaan haluttu verkkoliikenne päästetään läpi. Palomuuri estää lisäksi palveluihin kohdistuvat hyökkäykset sekä erilaisia reititys- ja lähdeosoitteen väärennykseen perustuvia hyökkäystapoja. (Viestintävirasto 2007a.)

Palomuuri siis suodattaa kaiken verkkoliikenteen ja oletusarvoisesti kieltää kaiken liikenteen. Suodatussäännöillä määritellään erikseen, mikä liikenne sallitaan ja mikä ei. Suodatussäännöt toimivat täten poikkeuksina oletussääntöön, jossa kaikki kielletään. Mikäli kaiken kieltävää oletussääntöä ei olisi, toimisi palomuuri ennemminkin reitittimen tavoin ja sallisi tällöin kaiken liikenteen. Termi *palomuuri* tulee rakennus- ja autoteollisuuden *seinä*-käsitteestä, joka viittaa palon leviämistä estävän seinän rakentamiseen. Palomuuri rakennuksen tai auton moottoritilassa tarkoittaa fyysistä estettä palon leviämiselle. Verkkoturvallisuudessa palomuuri toimii kuvainnollisesti samalla periaatteella ja mikäli palomuuri jostakin syystä lukittuu tai menee virhetilaan, estää se kaiken verkkoliikenteen. Tätä ominaisuutta kutsutaan vikaturvallisuudeksi. (Stewart 2011, 44–45.)

Perustavanlaatuisen tietoturvallisuuden saavuttamiseksi ajantasainen virustorjuntaohjelmisto ja vähintään ohjelmistopohjainen palomuuri ovat ehdottoman tärkeitä käyttöjärjestelmästä riippumatta. Haittaohjelmasta saastunut järjestelmä ei enää suojaa käyttäjän yksityisyyttä luotettavasti, eivätkä muut suojausmenetelmät ole silloin niin tehokkaita. Toisin kuin usein kuvitellaan, myös GNU/Linux- ja Mac OS X-käyttöjärjestelmille on tehty lukuisia haittaohjelmia. Esimerkiksi elokuussa 2012 löydettiin ensimmäinen salasanoja varastava troijalainen *BackDoor.Wirenet.1*, joka on suunnattu sekä GNU/Linux- että Mac OS X-käyttöjärjestelmille (Dr.Web 2012). Virustorjuntaohjelmistoja ja palomuuriohjelmistoja on saatavilla myös ilmaiseksi riisutumpina versioina, jotka ovat kuitenkin lähes yhtä tehokkaita kuin kaupalliset esikuvansa. Esimerkiksi tietoturvayhtiö Comodo tarjoaa virustorjuntaohjelmistoaan GNU/Linux-, Mac OS X- ja Windows-käyttöjärjestelmille sekä tehokasta palomuuriohjelmistoaan Windowsille (Comodo 2013). Ohjelmistot voi ladata Comodon kotisivuilta osoitteesta https://www.comodo.com.

Osa virustorjunta- ja palomuuriohjelmistoista tarjoaa lisäksi ns. hiekkalaatikkotilan turvattomien tiedostojen tai ohjelmien käyttämiseen. Hiekkalaatikkotilassa ohjelman käyttö rajataan ennalta määrätylle kiintolevyn alueelle, joka on mahdollista tyhjentää käytön jälkeen. Tämä mahdollistaa turvallisen tavan kokeilla epäilyttäviä ohjelmia tai verkkosivuja. Mikäli ohjelma tai verkkosivu sisältääkin haittaohjelmia, eivät ne hiekkalaatikkotilan ansiosta pääse tarttumaan pysyvästi järjestelmään. Windows-käyttöjärjestelmille on saatavissa kaupallinen, mutta ilmaiseksikin täysin toimiva, Sandboxie-sovellus hiekkalaatikkotilan luomiseen (Sandboxie 2013). Sandboxien voi ladata ohjelman kotisivuilta osoitteesta http://www.sandboxie.com.

Tietoturvayhtiöille ennestään tuntemattomia haavoittuvuuksia eli nollapäivähaavoittuvuuksia (engl. *zero-day exploit*) hyödyntävät hyökkäykset läpäisevät myös usein virustorjuntaohjelmistojen seulan. Tämän vuoksi virustorjuntaohjelmistot eivät tarjoa täyttä suojaa haittaohjelmilta, eikä käyttäjän kannata siksi tuudittautua osittain valheelliseen turvallisuuden tunteeseen. Tietoturvatuotteita on suositeltavaa käyttää, mutta samalla on hyvä ymmärtää

niiden rajallisuudet. Omilla toimillaan ja normaalilla varovaisuudella voi estää jo huomattavasti haittaohjelmien leviämistä järjestelmään.

3.2 Verkkoselaimet ja niiden lisäosat

Tietoverkkojen, kuten Internetin, selailua varten tarvitaan verkkoselainohjelma, joka hoitaa kommunikoinnin palvelinten ja käyttäjän koneen välillä. Verkkoselain tai yksinkertaisemmin selain on tietokoneohjelma, joka on tarkoitettu WWW-tietolähteiden (World Wide Web) noutamiseen, esittämiseen ja siirtämiseen. Verkkoselaimia ovat esimerkiksi Mozilla Firefox, Google Chrome, Internet Explorer, Safari ja Opera. Selaimen turvallisuuteen on hyvä kiinnittää huomiota, sillä huonosti konfiguroitu tai tunnetuille haavoittuvuuksille altis selain voi vaarantaa käyttäjän tietoturvan ja yksityisyyden suojan. Useat selaimet lähettävät oletuksena tietoja ohjelman käytöstä selaimen valmistajalle ja säilyttävät sivuhistoriatiedot. Yksityisyyden suojaamista ajatellen ylimääräiset tiedonlähetykset sekä historiatietojen säilyttäminen on turvallisempaa säätää asetuksista pois päältä. Selaimet saattavat lähettää verkkosivuille tietoja käyttäjän sijainnista ja kieliasetuksista, jotka on hyvä kytkeä pois selaimen asetuksista. Uudemmat selaimet mahdollistavat asetuksen, jonka kautta verkkosivuille lähetetään pyyntö siitä, ettei kävijä halua itseään seurattavan. Asetus ei kuitenkaan suojaa tarkkailulta, koska se toimii vain, mikäli palvelin tukee ja kunnioittaa pyyntöä.

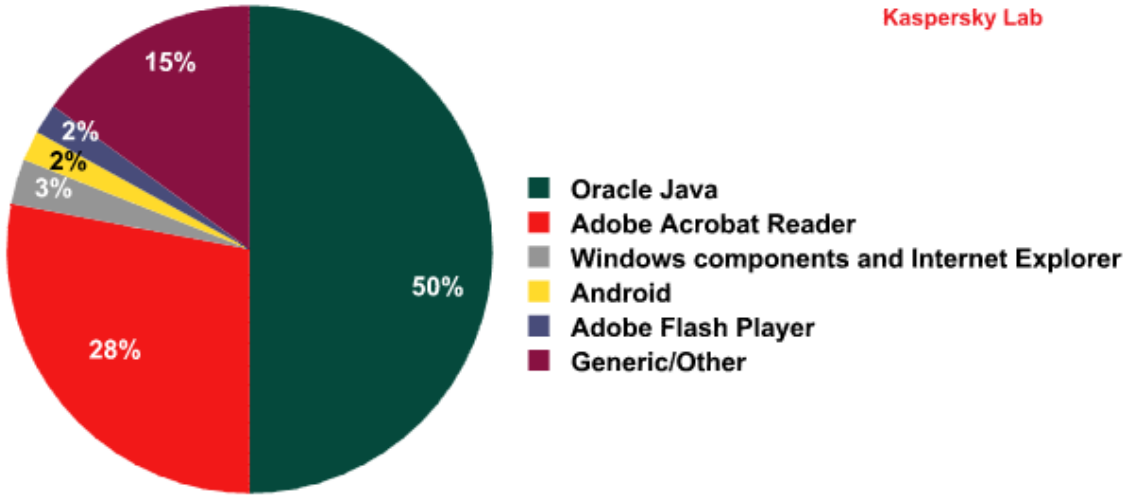
Nykyisin selaimet tukevat myös yksityistä selausta (engl. *incognito*), jolloin selain ei talleta käyttäjän sivuhistoriaa, hakuhistoriaa tai evästetietoja pysyvästi käytettävään laitteeseen. Yksityinen selaus -tila tarjoaa automaattisesti tapahtuvaa tiedon poistamista, minkä vuoksi tilan käyttäminen on järkevää. Käyttö ei kuitenkaan estä Internet-palveluntarjoajien tai verkkosivujen suorittamaa tarkkailua, mainosten kohdentamista, haittaohjelmien toimintaa eikä monia muita yksityisyyden suojalle haitallisia toimia. Tämän vuoksi yksityisyydestään huolehtivan on käytettävä lisäksi tehokkaampia keinoja.

Internetsivut saattavat asentaa käyttäjän tietokoneelle evästeitä eli keksitiedostoja (engl. *cookies*), joiden avulla käyttäjä voidaan esimerkiksi tunnistaa helposti seuraavalla vierailukerralla. Evästeiden avulla voidaan lisäksi tarkkailla käyttäjän toimia tai kohdentaa mainoksia. Nämä saattavat myös paljastaa käyttäjän identiteetin, minkä takia ne ovat riski yksityisyyden suojalle. Evästeet on mahdollista kieltää kokonaan selainten asetuksista tai asettaa selain kysymään lupa käyttäjältä joka kerta, kun jokin sivusto haluaa asentaa niitä. Turvallisinta olisi kieltää evästeet selaimen asetuksista kokonaan ja lisätä poikkeuksiin tarvittavat ja luotettavat sivustot, joiden selaaminen edellyttää evästeiden käyttöä. Tämän lisäksi selaimen voi säätää poistamaan evästetiedot sulkemisen yhteydessä.

Evästeiden lisäksi verkkosivut tai HTML-merkintäkieltä (*HyperText Markup Language*) sisältävät sähköpostiviestiviestit saattavat asentaa kuvapistetunnisteita (engl. *web bug*) käyttäjän koneelle. Näiden tarkoitus on seurata verkkosivustoissa tapahtuvia toimia tai sähköpostiviestin avaamista ja käyttöä. Ne ovat yleensä läpinäkyviä graafisia kuvia, jotka ovat yhden pikselin eli kuvapisteen kokoisia. Kuvapistetunnisteita voidaan estää tyhjentämällä selainten välimuistissa olevat verkkosisältötiedot sekä estämällä väliaikaistiedostojen pysyvä tallennus. Sähköpostiviestiohjelmat voidaan asettaa näyttämään sähköpostiviestit pelkästään tekstimuodossa, jolloin kuvapistetunnisteet eivät kopioidu käytettävälle koneelle.

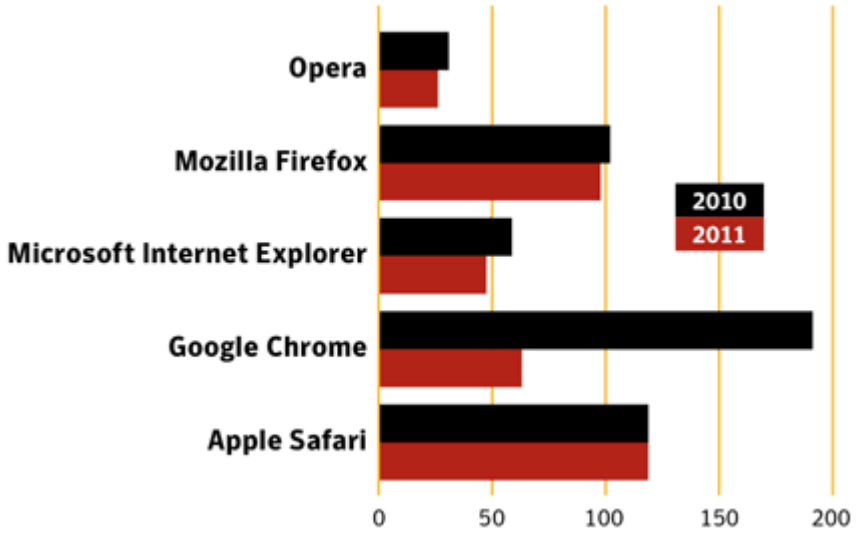
Osa www-sivuista käyttää erilaisia selainliitännäisiä (engl. *browser plug-in*) ja vaatii näitä toimiakseen kunnolla. Sellaisia ovat esimerkiksi Oracle Java-, Adobe Flash-, Microsoft ActiveX- ja Silverlight-liitännäiset. Nämä mahdollistavat monipuolisemman verkkosivujen sisällöntuottamisen, mutta sisältävät lisäksi omia haavoittuvuuksiaan, joiden kautta käyttäjän tietosuoja voi vaarantua haitallisilla verkkosivuilla. Tämän vuoksi nyrkkisääntönä voitaisiin pitää sitä, että liitännäisiä käytettäisiin vain tarvittaessa. (Dormann & Rafail 2008.) Usein selaimet tai liitännäisten automaattiset päivitystoiminnot ilmoittavat, jos liitännäisestä on uudempi versio tarjolla ja se pitäisi päivittää. Selainliitännäisten päivittäminen on tärkeää, koska päivitykset paikkaavat usein myös tietoturva-aukkoja.

Viime vuosina Java-selainliitännäisen haavoittuvuuksia on hyödynnetty ahkerasti hyökkäyksissä. Tietoturvayhtiö Kasperskyn (2012) raportoimat havainnot osoittavat, kuinka merkittäviä Javan haavoittuvuuksiin kohdistuvat hyökkäykset ovat muihin suhteutettuna. Kuviosta 1 voidaan nähdä, että Javan haavoittuvuuksia hyödyntävät hyökkäykset ovat varsin vakava uhkatekijä, koska ne käsittävät puolet (50 %) kaikista sovellusten haavoittuvuuksiin kohdistuneista verkkohyökkäyksistä. Javan haavoittuvuudet liittyvät yleensä Javan selainliitännäisiin eivätkä varsinaisiin työpöytäsovelluksiin. Javaan viitatessa voidaan myös tarkoittaa varsinaista ohjelmointikieltä tai ohjelmistoalustaan kuuluvaa ajoaikaista ympäristöä (engl. *Java Runtime Environment*). Javan selainliitännäinen on kuitenkin turvallisempaa poistaa käytöstä tai jättää kokonaan asentamatta.



Kuvio 3. Sovellusten haavoittuvuuksia hyödyntävien verkkohyökkäysten jakautuminen vuonna 2012 (Kaspersky 2012).

Selaimista itsestäänkin löytyy toisinaan uusia haavoittuvuuksia, jotka vaarantavat käyttäjän verkkohyökkäyksille. Haavoittuvuudet riskeeraavat käyttäjän yksityisyyden suojan, koska näitä hyödyntämällä hyökkääjä saattaa päästä suorittamaan haitallista koodia uhrikoneeseen. Kuvio 2 esittää tietoturvayhtiö Symantecin raportoimien haavoittuvuuksien määrää eri selaimissa vuosien 2010 ja 2011 aikana (Symantec 2012). Siitä voidaan nähdä, että haavoittuvuuksien määrä on pienentynyt miltei kaikissa tutkituissa verkkoselaimissa vuoden ajanjaksolla, mutta niitä on kuitenkin löytynyt useita edelleen.



Kuvio 4. Verkkoselainten haavoittuvuuksien määrä 2010–2011 (Symantec 2012).

Turvallisia selaimet eivät ole edelleenkään, sillä esimerkiksi maaliskuussa 2013 järjestetyssä Pwn2Own-tapahtumassa onnistuttiin löytämään pelkkiä selainten haavoittuvuuksia Chromen, Firefoxin ja Internet Explorerin uusimmista versioista (Kerner 2013). Tämän vuoksi selainten jatkuva päivittäminen uusimpiin versioihin on tärkeää. Selainten asetuksista olisi suositeltavaa asettaa automaattinen päivittäminen päälle, jotta käyttäjän ei tarvitsisi erikseen huolehtia päivitysten ylläpitämisestä.

Nykyaikaiset selaimet tukevat myös selainlaajennuksia (engl. *browser extension, Add-on*), joita hyödyntämällä tietoturvallisuutta ja yksityisyyden suojaa voidaan tehostaa. Suosituimpien selainten laajennukset ja asetukset on helppo säätää kerralla kuntoon menemällä osoitteeseen *fixtracking.com*, asentamalla sivuston suosittelemat laajennukset ja säätämällä suositellut asetukset selaimista käsin (DuckDuckGo 2013b). Mikäli verkkosivu tukee salausta HTTPS-protokollan kautta, kannattaa sitä käyttää. Verkkopankit ja luotettavat verkkokaupat tukevat tätä protokollaa, ja sivuilla vieraillessa kannattaakin tarkistaa, että yhteys on salattuna. Tämän voi varmistaa osoitepalkin alussa näkyvästä lukon kuvasta sekä HTTPS-tunnuksesta. Lisää HTTPS-protokollasta kerrotaan luvussa 4.3.

Eräs tarkoitukseen sopiva selainlaajennus on HTTPS Everywhere, joka on Electronic Frontier Foundationin ja The Tor Projectin yhteistyön tulos. Tällä selainlaajennuksella Firefox- ja Chrome-selaimet voivat automaattisesti hakea

salatun HTTPS-yhteyden, jos sivusto sellaista tarjoaa. (Electronic Frontier Foundation 2013a.) Mozilla-pohjaisille selaimille huomionarvoinen selainlaajennus on myös NoScript, joka oletusarvoisesti estää verkkosivujen käyttämät ohjelmakoodit ja lisäosat. Haittapuolena laajennuksella on se, että useat www-sivut eivät toimi sen jälkeen siten kuin ne on suunniteltu. Luotettaville sivuille voi kuitenkin antaa osittaiset tai täydet oikeudet, jolloin ne toimivat normaalisti. Selainlaajennuksen voi ladata osoitteesta http://noscript.net. (InformAction 2013.)

3.3 Salasanat

Salasanojen tarkoitus tietoturvassa on suojata tietoja ja mahdollistaa oikean henkilön pääsy suojattuun tietoon. Käyttäjänimet identifioivat käyttäjän, ja salasanat todistavat käyttäjän identiteetin oikeaksi. Siten salasanat varmistavat yksityisyyttä pitämällä arkaluontoiset tiedot salassa ulkopuolisilta. (Burnett & Kleiman 2006, 4.)

Ihmisluonto on sellainen, että emme pelkää uhkia, joita emme havaitse. Toisinaan on vaikea kuvitella, miksi joku haluaisi päästä sähköpostitiliimme tai mitä hyötyä kenellekään olisi päästä käsiksi tietoihimme, joita emme itse pidä kovinkaan arvokkaina. Tietoturvan tarpeen ja salasanojen tärkeyden aliarvioiminen onkin eräs suurimpia käyttäjän itsensä tekemiä virheitä. Eräs syy salasanojen murtamiselle saattaa olla hyökkääjän omien jälkien peittäminen tai naamioituminen toiseksi henkilöksi esimerkiksi roskapostin lähettämistä varten. Toisaalta hyökkäys voi olla vain yksi vaihe isommasta prosessista, jossa päämääränä on jokin arvokkaampi kohde. Se voi olla myös vain keino suorittaa kyseenalaisia liiketoimia, joissa päämääränä on huijata toisia tai päästä käyttäjän rekisteröitymiin maksullisiin palveluihin. Tosiasia on, että murrettujen salasanojen hyödyllisyyttä muille on toisinaan vaikea ymmärtää, mutta syitä suojaamiselle on. (Burnett & Kleiman 2006, 4, 12.)

Salasanojen selvittämiseen on useita tekniikoita, mutta niistä on hyvä tiedostaa yleisimmät, jotta voi suojautua niiden varalta. Helpoin tapa saada salasana

selville on yksinkertaisesti arvata se. Vaivattominta on arvata ensin oletusarvoisina olevat, yleisimmät ja käyttäjän henkilökohtaisiin tietoihin perustuvat salasanat, koska valitettavan usein käyttäjät eivät vaihda oletussalasanojaan tai käyttävät yksinkertaisia ja helposti arvattavia salasanoja. Erittäin huonoja salasanoja ovat myös lemmikkieläinten tai omien lasten nimet, jotka hyökkääjä voi nopeasti selvittää esimerkiksi sosiaalisen median kautta. Salasanojen arvaamista voidaan lisäksi nopeuttaa käyttämällä sanakirjahyökkäystä (engl. *dictionary attack*), jossa salasananmurto-ohjelmalla käydään läpi erilaisia sanalistoja. Monet salasanojen murtamiseen tarkoitetut ohjelmat pystyvät lisäksi yhdistelemään sanalistojen sanoja sekä kokeilemaan sanat myös takaperin. (Burnett & Kleiman 2006, 17.) Hyökkääjä voi luoda itse sanalistoja esimerkiksi käyttäjän henkilökohtaisten tietojen perusteella tai ladata valmiin listan Internetistä. Sanalistoja löytyy Internetistä useasta paikasta, esimerkiksi Kotimaisten kielten keskus tarjoaa 94 110 sanatietuetta sisältävän nykysuomen sanalistan kotisivuillaan (Kotimaisten kielten keskus 2007).

Sateenkaaritaulut (engl. *rainbow tables*) ovat ennalta laskettuja tauluja, jotka sisältävät tiivisteitä eli hajautusarvoja (engl. *hash*) miljardeista mahdollisista salasanoista. Näiden taulujen rakentaminen vie paljon aikaa, mutta valmiiden taulujen avulla hyökkääjä voi saada murrettua suuren määrän salasanoja muutamissa sekunneissa. Sateenkaaritaulut ovat tärkeitä murtamisessa, sillä niiden avulla kaikki alle 15 merkkiä sisältävät salasanat ovat haavoittuvia. (Burnett & Kleiman 2006, 18.)

Tehokkain keino salasanojen murtamiseksi on väsytysmenetelmä (engl. *brute force*), jossa käydään systemaattisesti läpi kaikki vaihtoehdot merkki merkiltä. Tekniikka on usein paljon aikaa vievä, joten sitä käytetään yleensä vasta viimeisenä keinona muiden tapojen jälkeen. (Burnett & Kleiman 2006, 18.) Tarpeeksi pitkä ja erikoismerkkejä sisältävä salasana antaa yleensä hyvän suojan tällaiselle hyökkäykselle, koska purkamiseen menisi tällöin nykyisellä laskentateholla suhteettoman kauan aikaa.

Salasanojen pituuden ja merkkiavaruuden suuruuden vaikutusta niiden turvallisuuteen voidaan tarkastella matemaattisten permutaatioiden avulla.

Permutaatioita voidaan muodostaa esimerkiksi tietokoneen näppäimistöstä. Suomalaisessa näppäimistössä on 29 kirjainta, 10 numeraalista merkkiä sekä 39 kuvavihjeillä olevaa, suhteellisen helposti kirjoitettavaa erikoismerkkiä (kuva 1).

Kuva 1. Suomalainen näppäimistö.

Salasanan erilaisten vaihtoehtojen määrä saadaan kaavalla a^n, jossa *a* on merkkiavaruuden suuruus ja *n* on salasanan pituus (Burnett & Kleiman 2006, 41). Esimerkiksi jos salasanan pituus olisi viisi merkkiä ja se koostuisi pienistä ja isoista kirjaimista (58) sekä numeroista (10), olisi laskukaava 68*68*68*68*68 eli 68^5. Näin ollen salasanan murtajan olisi käytävä läpi enintään 1 453 933 568 merkkiä. Vaikka puolitoista miljardia kuulostaa isolta luvulta, jopa nykyiset kuluttajaluokan tietokoneet pystyvät käymään läpi satoja miljoonia salasanoja sekunnissa hyödyntämällä mm. näytönohjainten laskentatehoa (InsidePro 2012). Toisekseen on hyvin epätodennäköistä, että salasana löytyisi vasta viimeisenä vaihtoehtona.

Taulukossa 1 on laskettu kuinka salasanan merkkien määrä ja käytetyt merkit vaikeuttavat murtamista. Taulukosta voidaan nähdä, että 10-merkkinen salasana, joka sisältää ainoastaan pieniä kirjaimia, onkin paljon tehokkaampi kuin seitsemänmerkkinen salasana, joka sisältää kaikkia suomalaisessa näppäimistössä näkyviä merkkejä. Käytännössä tämä tarkoittaa sitä, että vahvalta kuulostava *Y$äq~3P* onkin heikompi salasana väsytysmenetelmähyökkäykselle kuin esimerkiksi *ysokeepial*. Samalla tavalla kahdeksanmerkkinen erikoismerkkejä ja numeroita sisältävä salasana on

huomattavasti heikompi kuin 12-merkkinen salasana, joka sisältää pelkkiä pieniä kirjaimia.

Taulukko 1. Salasanan pituuden ja merkkien määrän vaikutus murtamisen kannalta.

Pituus	Vain pienet kirjaimet (29)	Kaikki näppäimistön merkit (107)
6	594 823 321	1 500 730 351 849
7	17 249 876 309	160 578 147 647 843
8	500 246 412 961	17 181 861 798 319 201
9	14 507 145 975 869	1 838 459 212 420 154 507
10	420 707 233 300 201	196 715 135 728 956 532 249
11	12 200 509 765 705 829	21 048 519 522 998 348 950 643
12	353 814 783 205 469 041	2 252 191 588 960 823 337 718 801
13	10 260 628 712 958 602 189	240 984 500 018 808 097 135 911 707
14	297 558 232 675 799 463 481	25 785 341 502 012 466 393 542 552 649
15	8 629 188 747 598 184 440 949	2 759 031 540 715 333 904 109 053 133 443

Hyökkääjä voi saada salasanan haltuunsa useilla eri tavoilla myös ilman varsinaista salasanan murtamista. Tämä onnistuu esimerkiksi käyttämällä näppäilyn tallentajaa (engl. *key logger*) tai snifferiä (engl. *sniffer*). Hyökkääjä voi myös hyödyntää selainten haavoittuvuuksia kaapatakseen salasanoja sisältäviä keksitiedostoja tai käyttää sosiaalisen manipuloinnin (engl. *social engineering*) keinoja. Näppäilyn tallentaja on vakoiluohjelma, joka tallentaa tietokoneen näppäimistön painallukset ja lähettää ne hyökkääjälle. Snifferi on puolestaan vakoiluohjelma, joka seuraa verkkoyhteyttä ja lähettää salaamattomat käyttäjätunnukset ja salasanat hyökkääjälle. Selaimista löydetään jatkuvasti uusia haavoittuvuuksia, joita hyökkääjä voi hyödyntää muun muassa varastamalla verkkosivujen tallentamia evästeitä (vrt. luku 3.2). Näiden lisäksi pahantahtoinen hyökkääjä voi käyttää sosiaalisen manipuloinnin keinoja eli esimerkiksi lähettää sähköpostin verkkopankin tai muun organisaation nimissä ja yksinkertaisesti pyytää salasanaa käyttäjältä. (Burnett & Kleiman 2006, 18–19.)

Salasanan valinnassa kannattaa pitää mielessä edellä mainitut murtamistavat. Salasanan ei tulisi löytyä mistään valmiista sanalistoista, sanakirjoista tai niiden yhdistelmistä. Toistamista sekä henkilökohtaisiin tietoihin perustuvia sanoja tulisi myös välttää. Salasanan pituus olisi hyvä olla vähintään 15 merkkiä, joihin kuuluu

sekä isoja että pieniä kirjaimia, numeroita ja erikoismerkkejä, jotta hyökkäysmenetelmistä saataisiin mahdollisimman tehottomia. Pääsääntönä on, että mitä pitempi ja laajempaan merkistöön perustuva salasana on, sen vaikeampi se on murtaa. Tekniikan edistyessä voidaan olettaa, että salasanojen pituutta joudutaan entisestään kasvattamaan, jotta niiden turvallisuus voidaan taata.

Salasanoja ja niitä sisältäviä palvelimia murretaan päivittäin, minkä vuoksi salasanojen säännöllinen vaihtaminen on myös erityisen tärkeää. Samaa salasanaa ei ole järkevää käyttää useassa paikassa, koska jos joku palvelu murretaan, pääsee hyökkääjä samalla kertaa muihinkin tietoihin käsiksi. Salasanoja ei tule koskaan luovuttaa sähköpostilla tai sosiaalisen median kautta tulleilla kyselyillä. Ajantasaisen virusturvan ja palomuurin käyttäminen on tärkeää, jotta haittaohjelmien ja näppäinten tallentajien uhat pienenevät (vrt. luku 3.1). Haittaohjelmien ja tietoturva-aukkojen estämiseksi myös käyttöjärjestelmän, selainten sekä selainliitännäisten ja -laajennusten päivityksistä on syytä pitää huolta (vrt. luku 3.2).

Näppäilyn tallentajia voidaan estää myös käyttämällä erillisiä ohjelmia tai selainlaajennuksia, jotka käyttävät virtuaalista näppäimistöä, jolloin haittaohjelmat eivät saa tärkeitä tietoja tallennettua. Esimerkiksi ilmainen, Windows-käyttöjärjestelmillä toimiva Neo’s SafeKeys -ohjelma tarjoaa käyttäjälle virtuaalisen näppäimistön, jolta tieto voidaan siirtää raahaamalla se haluttuun paikkaan ilman leikepöydälle tallentamista. Tällöin näppäilyn tallentaja -ohjelma ei voi kaapata salasanaa näppäimistöstä tai leikepöydältä. Tämän lisäksi ohjelma poistaa päällä ollessaan myös kuvakaappauksen eli näytön näkymän tallentamisen käytöstä. (Aplin Software 2012.) Näppäilyn tallentajia vastaan on olemassa myös tehokkaampia ja automaattisesti taustalla toimivia sovelluksia. Windows-käyttöjärjestelmillä toimivia ovat esimerkiksi QFX Software KeyScrambler, Zemana AntiLogger ja SpyShelter Stop-Logger (QFX Software Corporation 2013, Zemana 2013, SpyShelter 2012). Nämä kaupalliset, mutta ilmaisenakin toimivat ohjelmat, tarjoavat mm. näppäilyn salaamista tunnetuilla salausalgoritmeilla, leikepöydän turvaamista, ruudunkaappausten estämistä ja webkameroiden tallentamisen suojausta. Edellä mainittujen ohjelmien käyttö on

suositeltavaa varsinkin julkisissa tietokoneissa, joiden suojauksesta ei ole mitään takeita.

Käyttäjätilien murtaminen saadaan huomattavasti vaikeammaksi, jos käytetään kaksiosaista tai kolmiosaista todentamismenetelmää (engl. *two-factor authentication, three-factor authentication*). Menetelmistä käytetään myös nimitystä vahva tunnistaminen (engl. *strong authentication*) ja ne perustuvat siihen, että käyttäjällä on käytössään seuraavista kaksi tai useampi todiste itsensä identifioimiseen: 1) jotain, minkä vain käyttäjä tietää, kuten salasana, 2) jotain, minkä vain käyttäjä omistaa, kuten matkapuhelin tai avaintiedosto, 3) jotain uniikkia tietoa käyttäjästä, kuten esimerkiksi sormenjälki. (RSA 2012.) Osa verkkopalveluista (mm. Google ja Dropbox) onkin jo ottanut kyseistä tekniikkaa käyttöönsä.

Salasanojen turvallinen rakentaminen ja niiden muistaminen käy kuitenkin lähes mahdottomaksi tehtäväksi, kun eri palveluihin tarvittavien salasanojen määrä kasvaa. Salasanojen satunnaista luomista, niiden listaamista sekä tehokasta ja helppoa käyttöä varten on siksi rakennettu useita ohjelmia ja palveluita. Näistä salasanojen hallintasovelluksista mainitsemisen arvoisia ovat avoimeen lähdekoodiin perustuvat Password safe- ja KeePass-ohjelmat sekä kaupallinen LastPass-verkkopalvelu (Password Safe 2013, KeePass 2013, LastPass 2013). Näissä käyttäjä voi ottaa lisäksi vahvan tunnistamisen menetelmän käyttöönsä, ja tällöin muistettavana on enää yksi salasana, jonka avulla pääsee käsiksi muihin salasanoihin. Salasanan lisäksi käyttäjä voi siis hyödyntää varmennuksessa esimerkiksi muistitikulla pidettävää avaintiedostoa, jolloin turvallisuustaso nousee.

3.4 Tietojen salaaminen

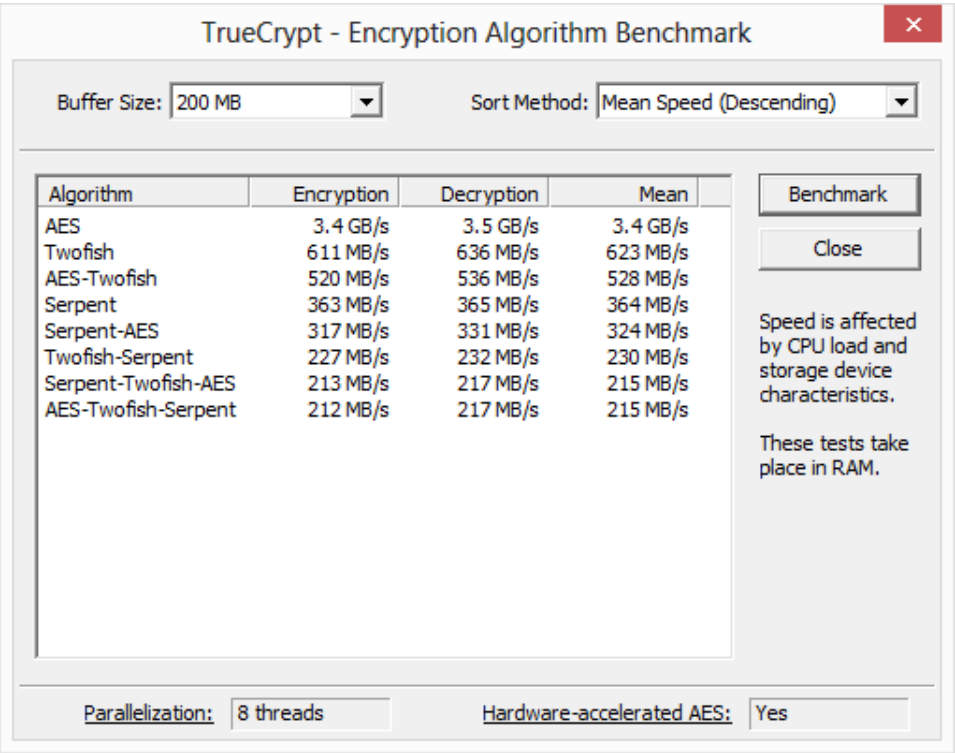
Salausmenetelmien tarkoituksena on varmistaa, että tiedot säilyvät luottamuksellisina, eheinä ja kiistämättöminä. Niiden tavoitteena on luoda salaus, jonka murtaminen kohtuullisessa ajassa ja kohtuullisin resurssein on mahdotonta. Kohtuullinen aika ja resurssit riippuvat salatun tiedon tärkeydestä. Vahvoiksi salausmenetelmiksi kutsutaan sellaisia menetelmiä, joiden

murtaminen nykyisin saatavissa olevilla laskentaresursseilla on mahdotonta tai erittäin vaikeaa. Nykyisillä tietokonelaitteilla vahvojen salausmenetelmien käytölle ei ole varsinaista estettä, koska niiden laskentakapasiteetti mahdollistaa salausten helpon ja nopean käytön. Kun salausmenetelmä on toteutettu oikein, voidaan salaus purkaa vain käymällä läpi koko salausmekanismin avainavaruus ja kokeilemalla kaikkia mahdollisia salausavaimia. (Viestintävirasto 2009.)

Kiintolevyn ja varsinkin siellä olevien henkilökohtaisten asiakirjojen salaaminen on merkittävä suojauskeino tietoturvauhkien suhteen. Vaikka hyökkääjä pääsisi laitteessa oleviin tietoihin käsiksi fyysisesti tai verkon kautta takaportin avulla, estää tehokas salaaminen tärkeisiin tietoihin pääsyn. Salaaminen tarjoaa tietoturvan myös varkauden sattuessa, jolloin varas ei pääse käsiksi tärkeisiin dokumentteihin.

Tietojen salaaminen onnistuu helposti sekä kaupallisilla että ilmaisilla vapaan lähdekoodin ohjelmilla. Microsoft Windows -käyttöjärjestelmässä kiintolevyn tai sen osioiden salaus onnistuu mm. TrueCrypt- tai DiskCryptor-ohjelmilla, jotka perustuvat vapaaseen lähdekoodiin (TrueCrypt Foundation 2013, DiskCryptor 2013). TrueCrypt-ohjelmisto toimii myös GNU/Linux- ja Mac OS X -käyttöjärjestelmillä. Sen voi ladata ilmaiseksi ohjelman kotisivuilta osoitteesta http://www.truecrypt.org. (TrueCrypt Foundation 2013.)

Ohjelman lataamisen ja asentamisen jälkeen sillä voidaan tehdä nopeustestit eri salausmenetelmille valitsemalla ohjelman valikosta *Tools* ja sieltä *Benchmark*. Kuten kuvasta 2 voidaan nähdä, on AES-salausmenetelmä selvästi nopein ratkaisu ja siksi usein järkevin vaihtoehto salaukselle. Kuvassa 2 näkyvässä nopeustestissä on käytetty laitteistotasolla AES-salausta tukevaa prosessoria, jolloin nopeusero on vielä selkeämmin nähtävissä.

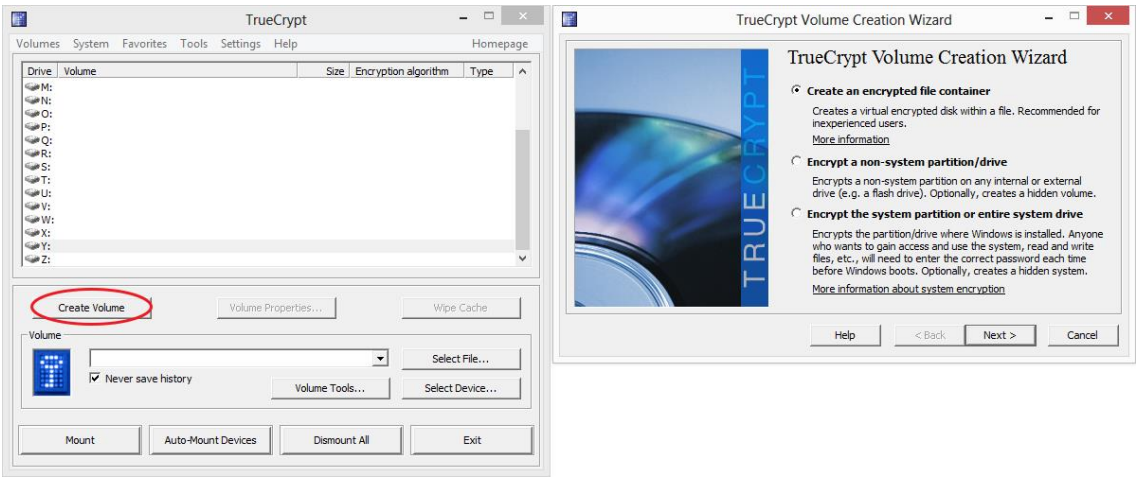


Kuva 2. Kuvakaappaus TrueCryptin salausmenetelmien nopeustestistä (TrueCrypt Foundation 2013).

AES (*Advanced Encryption Standard*) on Yhdysvaltojen hallituksen hyväksymä salausstandardi, jota käytetään laajalti eri ohjelmistojen, verkkoliikenteen, henkilötietojen ja organisaatioiden IT-infrastruktuurin suojelemiseen. AES on symmetrinen lohkosalausmenetelmä, joka salaa ja purkaa tiedon useiden kierroksien läpi. Käytettävien kierrosten lukumäärä (10, 12 tai 14) riippuu käytetyn avaimen pituudesta (128-bittinen, 192-bittinen tai 256-bittinen). Uudet prosessorit tukevat AES-NI-käskykantaa (*Advanced Encryption Standard New Instructions*), joka nopeuttaa huomattavasti salausta ja purkua. (Rott 2012.) TrueCrypt tukee prosessorien AES-NI-käskykantaa, ja uudemmilla prosessoreilla AES-salauksen käyttäminen on nopeushyödyn vuoksi kannattavaa.

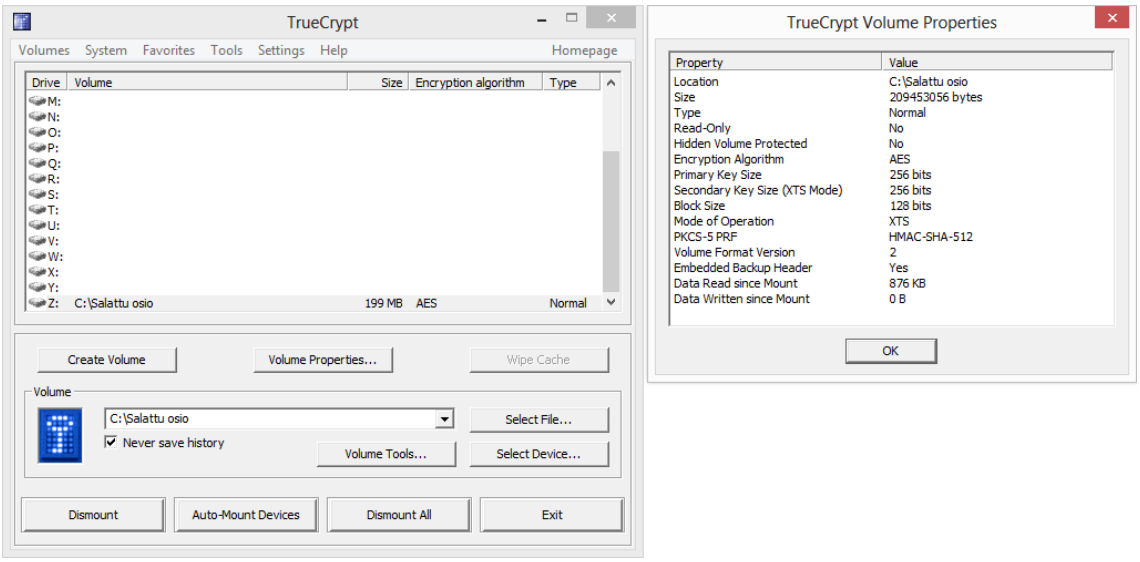
TrueCryptillä voidaan salata koko kiintolevy tai sen osio, luoda salattu ja piilotettu kiintolevyn osio tai luoda salattu tiedostosäilö, jota käytetään levyosion tapaan. Seuraavaksi käydään läpi, miten ohjelmalla luodaan tiedostosäilö 256-bittisellä AES-salauksella ja miten sitä käytetään. Ennen salauksen luomista on hyvä muistaa, että tehokkaan salauksen jälkeen salattuihin tiedostoihin ei enää pääse käsiksi, jos salasanan unohtaa.

Ohjelman käynnistämisen jälkeen valitaan kuvassa 3 näkyvä *Create Volume* -painike, joka käynnistää osion luomisen. Tämän jälkeen avautuu salausosion ohjattu toimintoikkuna. Siitä valitaan *Create an encrypted file container* -toiminto, jolla salattu tiedostosäilö luodaan. Seuraavasta näkymästä valitaan tiedostosäilön muodoksi oletuksena oleva *Standard TrueCrypt volume* ja jatketaan. Tämän jälkeen valitaan tiedoston sijainti ja nimi *Select File…* -painikkeella. Nimeksi ja tiedoston sijainniksi voidaan laittaa halutut tiedot. Seuraavassa ikkunassa valitaan *Encryption Algorithm* -valikosta salausalgoritmiksi AES ja *Hash Algorithm* -valikosta tiivisteeksi SHA-512. Ohjelma käyttää valittua tiivistealgoritmia satunnaislukugeneraattorissaan. Sen jälkeen valitaan tiedostosäilön koko, esimerkiksi 200 MB eli 200 megatavua. Seuraavaksi kirjoitetaan salasana ja varmistetaan kirjoittamalla se toiseen kertaan. Tässä kohdassa voidaan valita lisäksi avaintiedosto, joka mahdollistaa kaksiosaisen todentamismenetelmän hyödyntämisen (vrt. luku 3.3). Tämän jälkeen voidaan edetä seuraavaan näkymään, jossa ohjelman satunnaislukugeneraattori luo satunnaista tietoa, jolla salataan tiedostosäilö. Kun hiirtä liikuttelee edestakaisin ohjelman ikkunan kohdalla, salausavainten kryptografinen vahvuus suurenee. Samasta ikkunasta voidaan valita myös tiedostojärjestelmän tietoja, mutta oletusarvoiset käyvät hyvin. Lopuksi valitaan *Format*-painike, jolloin ohjelma luo tiedostosäilön. Kun luonti on onnistunut, voi ohjatun toiminnon lopettaa.



Kuva 3. Kuvakaappaus uuden salauslohkon luomisesta TrueCrypt-ohjelmalla (TrueCrypt Foundation 2013).

Salatun tiedostosäilön voi nyt liittää järjestelmään valitsemalla kirjaintunnus asemalle, etsimällä salattu säilö *Select File…* -painikkeella ja lopuksi painamalla *Mount*, joka liittää säilön tiedostojärjestelmään. Tämän jälkeen ohjelma kysyy salasanaa, jonka syöttämisen jälkeen osio toimii muiden kiintolevyosioiden tapaan. Tiedostosäilön tiedot voidaan tarkastaa valitsemalla *Volume Properties*.. kuvan 4 mukaisesti. Käytön jälkeen säilön voi sulkea valitsemalla *Dismount*.



Kuva 4. Kuvakaappaus TrueCryptillä liitetyn tiedostosäilön ominaisuuksista (TrueCrypt Foundation 2013).

Osa käyttöjärjestelmistä tukee myös sisäänrakennettuna kiintolevyn salausta. Microsoft Windows 7 Ultimate- ja Enterprise- sekä Windows 8 Pro- ja Enterprise-versiot tukevat Microsoftin omaa BitLocker-salausta. Applen Mac OS X Lion tai sitä uudemmilla versioilla voi puolestaan kiintolevyn salata käyttämällä FileVault 2 -metodia. Myös useat GNU/Linux-distribuutiot ovat tukeneet kiintolevyn LUKS-salausta (*Linux Unified Key Setup*) jo vuosia. (Lee 2012.)

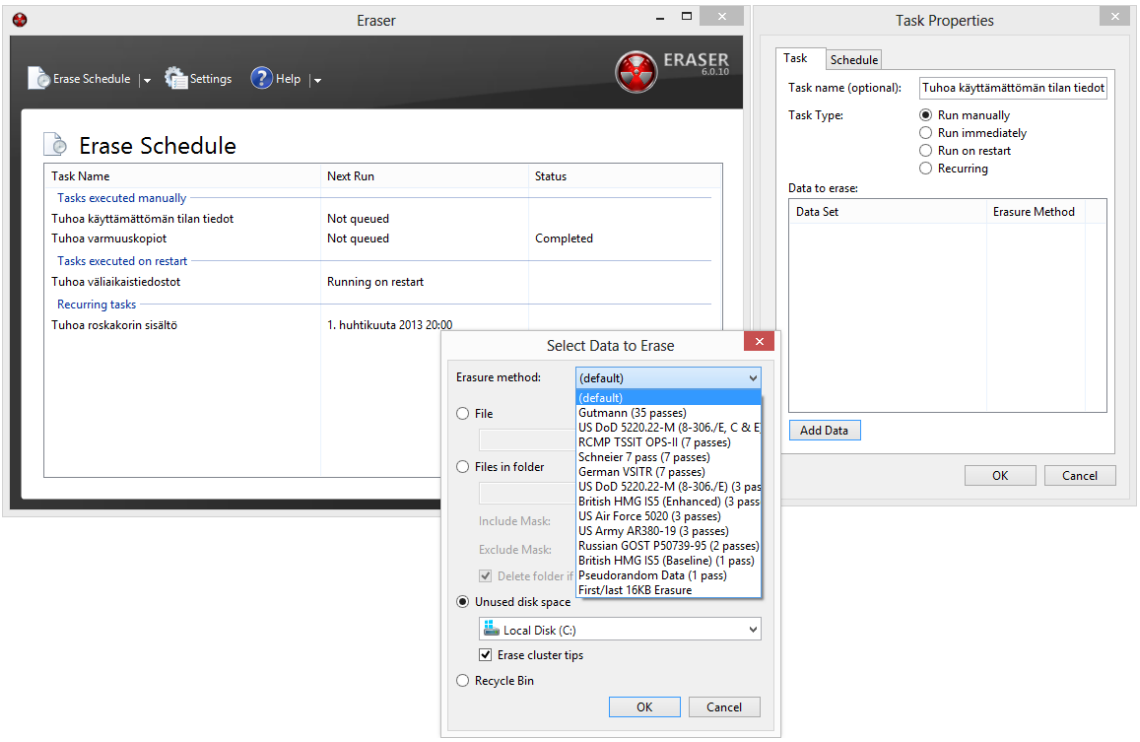
Yksityisyyden suojan kannalta arkaluontoiset tiedot on oleellista salata tehokkaalla salausmenetelmällä. Arkaluontoisiksi tiedoiksi voitaisiin ajatella tietoja, joiden ei haluaisi joutuvan vapaaseen levitykseen Internetiin. Nykyisillä tietokoneilla tiedon salaaminen on myös tarpeeksi nopeata, jolloin suurta haittaa salauksesta ei ilmene. Koko järjestelmän salaaminen puolestaan osoittautuu hyödylliseksi erityisesti varkauden sattuessa, ja varsinkin nopeammilla tietokoneilla se on edullinen ja kannattava varmuustoimenpide.

3.5 Tiedonhävitys

Tietokoneen tietojen varastoinnin suunnittelussa pääsääntönä on ollut suojata käyttäjän tiedot hinnalla millä hyvänsä. Tietojärjestelmien ensisijaisina massamuisteina toimivat levyasemat on suunniteltu siten, että ne estävät vahingossa poistettujen tietojen tuhoamisen. Käyttöjärjestelmät puolestaan estävät tietojen lopullista tuhoutumista erilaisilla tekniikoilla, kuten roskakori-kansioilla ja tietojenpalautuskomennoilla. (Hughes & Coughlin 2008.)

Normaali tiedoston poistaminen katkaisee ainoastaan tiedoston ja tiedostojärjestelmän välisen linkin, muttei poista varsinaista tiedoston sisältöä. Tämä tarkoittaa sitä, että tiedoston sisältö jää talteen levysektoreihin ja häviää vasta silloin, kun käyttöjärjestelmä kirjoittaa uutta tietoa samojen levysektoreiden päälle. Pelkän tiedostoon viittaavan linkin poistaminen on kuitenkin huomattavasti nopeampaa kuin koko tiedoston pysyvästi poistaminen päällekirjoittamalla. Tämän lisäksi levyasemat suojaavat tietojen lopullista häviämistä siten, että ne käyttävät tiedostojen palauttamiseen virheidenhavaitsemis- ja korjaamistekniikkaa, jotta ne eivät palauttaisi vääriä tietoja. Kaikesta tästä voidaankin päätellä, että tiedostojen lopullinen poistaminen on epänormaali tapahtuma ja että turvallinen poistaminen vaatii käyttäjältä erityisiä toimenpiteitä. (Hughes & Coughlin 2008.)

Tietojen hävitystä varten on olemassa useita eri sovelluksia, mutta tietojen lopullinen tuhoaminen onnistuu myös ilmaisilla ohjelmilla. Windows-käyttöjärjestelmälle on tarjolla esimerkiksi Eraser-sovellus, jolla tiedot voidaan poistaa lopullisesti käyttämällä suosittuja menetelmiä tiedon ylikirjoittamiselle (kuva 5). Ohjelman voi ladata ilmaiseksi osoitteesta http://eraser.heidi.ie. (Eraser 2013.)



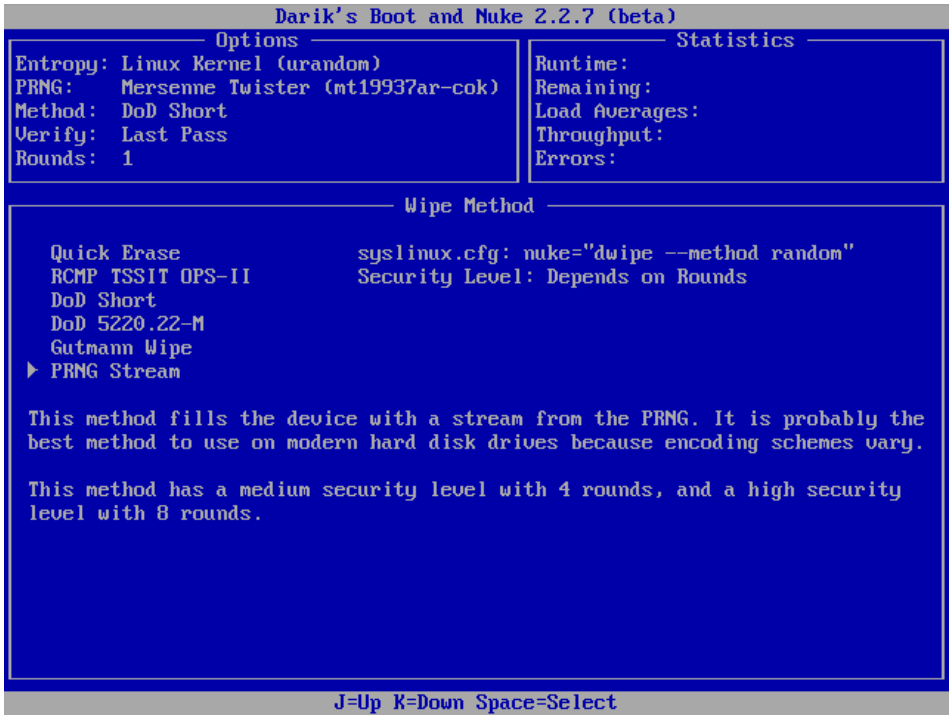
Kuva 5. Kuvakaappaus ajastuksen lisäämisestä tietojen poistamiselle Eraserilla (Eraser 2013).

Seuraavaksi käydään läpi, kuinka Eraser-sovelluksella voidaan hävittää tietoja turvallisesti. Eraserissa tiedostojen poiston tapahtumat luodaan ohjelman pääikkunassa valitsemalla hiiren oikealla napilla *New Task*. Tämän jälkeen tapahtumalle voidaan antaa nimi ja valita, milloin se suoritetaan. Suoritusajankohta voidaan valita manuaalisesti käynnistettäväksi, heti tehtävän lisäyksen jälkeen suoritettavaksi, koneen käynnistyksen yhteydessä tai erikseen määritettynä aikana tapahtuvaksi. Poiston kohde valitaan *Add Data* -toiminnolla. Avautuvasta ikkunasta voidaan valita tiedonhävityksen kohde ja mitä menetelmää tuhoamiseen käytetään. Tämä tarkoittaa lähinnä sitä, kuinka monta kertaa ja millä tavoin uusi merkityksetön tieto kirjoitetaan vanhan poistettavan tiedon päälle. Menetelmän valinnassa perussääntönä voi ajatella, että kolme tai seitsemän kertaa ylikirjoitettu data on useimmiten mahdotonta palauttaa. Usein myös poistamiseen kuluvalla ajalla on merkitystä, sillä mitä useammin tiedon päälle kirjoitetaan, sen kauemmin poistamisessa kestää. Nopeus on suhteellinen tietokoneen ja ylikirjoitettavan laitteen suorituskyvyn kanssa.

Linux-käyttäjille tiedonpoistamista varten on olemassa esimerkiksi Scrub-työkalu, jonka avulla tieto voidaan tuhota useilla ylikirjoitusmenetelmillä. Työkalun voi

ladata lähdekoodeineen osoitteesta https://code.google.com/p/diskscrub. (Diskscrub 2013.) Mac OS X -käyttäjät voivat puolestaan käyttää Applen omaa Disk Utility -ohjelmaa, joka tukee myös useita tiedon ylikirjoitusmenetelmiä.

Kokonaisten kiintolevyjen (engl. *Hard Disk Drive*) ja SSD-levyjen (engl. *Solid State Drive*) tietojen poistamiseen on tarjolla Darik's Boot and Nuke eli DBAN-niminen ohjelmisto (kuva 6). Ohjelmiston voi ladata ilmaiseksi osoitteesta http://sourceforge.net/projects/dban. (Darik's Boot And Nuke 2013). DBANilla poistaminen onnistuu polttamalla ladattava ISO-levykuva cd- tai dvd-levylle. Vaihtoehtoisesti levykuvan voi asentaa muistitikulle, josta on tehty käynnistävä asennusmedia. Tämän jälkeen ohjelmisto käynnistetään tietokoneen käynnistymisen yhteydessä suoraan valitulta asennusmedialta.



Kuva 6. Kuvakaappaus DBAN-ohjelman ylikirjoitusmenetelmän valinta -kohdasta (Darik's Boot And Nuke 2013).

DBAN tukee useita tehokkaita poistometodeita, jolloin tiedon palauttamisesta tulee mahdoton tehtävä. Vanhojen tietojen poistaminen tallennuslaitteilta on erityisen tärkeää yksityisyyden suojan kannalta, ja DBANin käyttö onkin tarpeellista esimerkiksi vanhan tallennusmedian käytöstä poistamisen yhteydessä tai sen jälleenmyynnissä.

Tarpeettoman mutta arkaluontoisen tiedon turvallinen tuhoaminen on edellytys hyvälle tietoturvalle. Tiedot voidaan tietysti tuhota tehokkaasti myös hajottamalla tallennusmedia fyysisesti. Kiintolevyt voidaan tuhota esimerkiksi voimakkaiden magneettikenttien avulla, ja SSD-levyt voidaan hajottaa käyttökelvottomiksi vasaroimalla sisällä olevat virtapiirit. Fyysinen tuhoaminen on kuitenkin yleensä yliampuva toimenpide ja ohjelmallisesti useaan kertaan ylikirjoitettua tietoa voidaan jo pitää tarpeeksi turvallisena tiedonhävityksenä.

4 Olennaiset verkkoprotokollat

Tietoliikenteen salaamisella tarkoitetaan datan eli digitaaliseksi muunnetun tiedon siirtämisen salaamista lähettäjältä vastaanottajalle. Seuraavissa alaluvuissa käsitellään erilaisten verkkoprotokollien ja tekniikoiden hyödyntämistä turvallisessa ja salatussa tiedonsiirrossa. Protokolla on menettelytapa tai standardi, joka määrittelee tai mahdollistaa yhteydet laitteiden tai ohjelmien välillä.

Ensin kuvataan lyhyesti yleisellä tasolla tietoverkkoprotokollien kokonaisuus, minkä jälkeen paneudutaan tietoliikenteen salaamisen kannalta merkittäviin protokolliin. Pääpaino luvun asioissa on Internet-selailun ja tiedonsiirron salaamisessa erilaisia protokollia ja menetelmiä hyödyntäen. Tarkoitus on käsitellä muutamia protokollia ja menetelmiä, joiden avulla esimerkiksi www-sivujen selailu voidaan suojata ulkopuoliselta tarkkailulta. Seuraavissa alaluvuissa esiteltyjen protokollien ja seikkojen tarkoitus on auttaa ymmärtämään laajemmin muissa luvuissa esiteltäviä asioita.

4.1 TCP/IP

Internet-liikenteessä käytetään usean tietoverkkoprotokollan yhdistelmää, johon viitataan lyhenteellä TCP/IP (*Transmission Control Protocol / Internet Protocol*). Nimi juontuu siitä, että kyseiset protokollat olivat ensimmäiset ja tärkeimmät

standardia käyttävät protokollat. Arkkitehtuurin kuvaamiseen käytetään viitemalleja, jotka hahmottavat paremmin yhdistelmän kerrosten toimintaa. Näitä ovat esimerkiksi viitemallit, kuten TCP/IP ja OSI (*Open Systems Interconnection Seven-Layer Reference Model*). Viitemallit vaihtelevat yleensä kolmen ja seitsemän kerroksen välillä riippuen niiden kuvaajasta. Taulukossa 2 on kuvattu viiden kerroksen TCP/IP-malli. (Comer 2009, 5–15.)

Taulukko 2. TCP/IP-viitemallin kuvaus ja kerrosten esimerkit (Comer 2009, 9).

Kerros	TCP/IP-malli	Kerrokseen kuuluvat mm.
Kerros 5	Sovelluskerros (*Application Layer*)	HTTP, TLS/SSL, SSH, DNS
Kerros 4	Kuljetuskerros (*Transport Layer*)	TCP, UDP, RTP
Kerros 3	Verkkokerros (*Internet Layer*)	IP (IPv4, IPv6), IPsec
Kerros 2	Siirtoyhteyskerros (*Network Interface Layer/Data Link Layer*)	L2TP, PPP, DSL
Kerros 1	Fyysinen kerros (*Physical Layer*)	Reititin, lähetystaajuudet

TCP/IP-mallin sovelluskerros määrittelee sovellusten vuorovaikutuksen niiden kommunikoidessa. Sen piiriin kuuluvat mm. sähköpostin, tiedonsiirron, verkkoselailun, pikaviestinnän ja videopuheluiden protokollat. Kuljetuskerroksen protokollat puolestaan tarjoavat tietokoneen sovellukselle yhteyden toisen tietokoneen sovellukseen. Ne määrittelevät mm. vastaanotetun datan tiedonsiirtonopeuden, verkkoruuhkia estävät mekanismit sekä tekniikoita, jotka tarkistavat, että kaikki data vastaanotetaan oikeassa järjestyksessä. Verkkokerroksen protokollat sen sijaan muodostavat olennaisen perustan Internetille. Siihen kuuluvat protokollat määrittelevät tietokoneiden välisen viestinnän Internetin kautta, Internetin osoiterakenteen sekä Internetissä liikkuvien pakettien muodon. Ne valitsevat myös menetelmän suurien pakettien jakamiseksi pienempiin eriin siirtoa varten sekä virheiden raportointiin kuuluvat mekanismit. Siirtoyhteyskerroksen protokollat määrittelevät yksityiskohdat ylempien kerrosten protokollien viestinnälle. Näitä ovat esimerkiksi tekniset tiedot verkko-osoitteista ja pakettien maksimikoosta, jota verkko voi tukea. Alimmaisena kerroksena fyysinen kerros sisältää taustalla olevat lähetyksen välineet sekä laitteiston. (Comer 2009, 10.) Fyysisen kerroksen protokollat eivät

kuitenkaan varsinaisesti kuulu TCP/IP-protokollaperheeseen, mutta ne ovat toisinaan mukana viitemallin kuvauksessa.

Kerrosmallit eivät ole pelkästään abstrakteja käsitteitä, jotka auttavat ymmärtämään protokollia. Sen sijaan protokollatoteutukset jäljittävät kerrosmalleja siirtämällä tiedot eteenpäin seuraavaan kerrokseen. Tässä tutkielmassa käsitellään lähinnä sovelluskerrokseen, kuljetuskerrokseen ja verkkokerrokseen kuuluvia protokollia ja ratkaisuja. Tämän alaluvun tarkoituksena oli hahmottaa hieman verkkoprotokollien yhtenäisyyttä ja antaa selkeämpi kokonaiskuva tilanteesta.

4.2 SSL/TLS

Verkkoturvallisuuteen on saatavilla useita erilaisia menettelytapoja, jotka tarjoavat siirrettävän tiedon salausta, mutta eroavat toisistaan mm. sijainniltaan TCP/IP-viitekehyksessä. Eräs yleisimmistä tavoista suojata liikennettä on SSL-protokolla (*Secure Sockets Layer*) ja sen seuraaja TLS-protokolla (*Transport Layer Security*). SSL oli alun perin Netscape-verkkoselaimeen kehitelty salausprotokolla ja sen tarkoitus oli turvata salaamattoman TCP-protokollan heikkoudet. Kolmas versio SSL-protokollasta suunniteltiin julkiselle tarkastelulle ja siitä julkaistiin Internetissä asiakirjaluonnos. Myöhemmin protokollan perustamisesta Internet-standardiksi päästiin yksimielisyyteen, ja sitä kehittämään perustettiin TLS-työryhmä. Ensimmäistä julkaistua TLS-versiota voidaankin pitää SSLv3.1-versiona ja se on hyvin samankaltainen ja yhteensopiva SSLv3-version kanssa. (Stallings 2011, 487–489.)

TLS ja SSL-protokollat salaavat verkkoyhteyksien osuudet TCP/IP-mallin sovelluskerroksella, josta ne siirtyvät kuljetuskerrokselle. Taulukko 3 (Stallings 2011) kuvaa protokollien välisen yhteyden. (Stallings 2011, 488.)

Taulukko 3. TLS/SSL sijoittuminen TCP/IP-viitekehyksessä (Stallings 2011, 488).

HTTP	FTP	SMTP
SSL tai TLS		
TCP		
IP		

SSL/TLS-protokollaa voidaan käyttää joko osana taustalla olevaa tietoverkkoprotokollien yhdistelmää tai se voidaan sisällyttää ohjelmistojen hyödyntämiin erillisiin paketteihin. (Stallings 2011, 488.) Nykyisin protokollan versiot ovat levinneet laajaan käyttöön ja niitä tukevat mm. selaimet, sähköpostiohjelmat ja pikaviestimet.

4.3 HTTP ja HTTPS

HTTP-protokolla (*Hypertext Transfer Protocol*) eli hypertekstin siirtoprotokolla toimii perustana www-palvelinten ja selainten väliselle tietoliikenteelle. Protokolla käyttää salaamatonta TCP-protokollaa yhteyden muodostamiseen palvelimen ja selaimen välillä ja on siksi altis tiedon sieppaukselle ja salakuuntelemiselle. HTTPS on muutoin sama sovellusprotokolla kuin HTTP, mutta se tunneloidaan turvallisen TLS-salausprotokollan läpi (vrt. luku 4.2). Tämä suojaa viestiliikennettä ja takaa tietojen eheyden verkossa, mikä vähentää salakuuntelun mahdollisuuksia. HTTP-pyynnöt ja -vastaukset toimivat kuitenkin täsmälleen samalla tavalla riippumatta siitä, käytetäänkö SSL-salausta vai ei. (Stuttard & Pinto 2011, 49.)

Sekä TLS- että SSL-protokollan käyttämistä HTTP-protokollan yli kutsutaan nimellä HTTPS (*Hypertext Transfer Protocol Secure*). HTTPS-ominaisuus on sisäänrakennettuna kaikissa moderneissa selaimissa ja sen käyttö riippuu verkkopalvelimen tuesta. Sivuston käyttämän protokollan huomaa sen verkko-osoitteesta eli URL:stä (*Uniform Resource Locator*). (Stallings 2011, 506–507.) Yleisesti käytettävä ja Internetissä vakiintunut URL-osoitteen muoto on *protokolla://tietokoneen_nimi:portti/dokumentin_nimi%parametrit*. Protokollalla tarkoitetaan protokollaa, jolla päästään dokumenttiin käsiksi. Tietokoneen nimellä

tarkoitetaan IP-osoitetta eli Internet-protokollan osoitetta tai verkkotunnusta eli domain-nimeä, joka osoittaa dokumentin sisältävään tietokoneeseen. Protokollan käyttämä porttinumero (*:portti*) on valinnainen lisätieto, joka kertoo palvelimen käyttämän portin. *Dokumentin_nimi* viittaa palvelimella olevaan asiakirjaan ja *%parametrit* antavat valinnaisia lisäparametreja verkkosivulle. Siksi verkko-osoitteet *http://www.yksityisyydensuoja.fi:80/index.html* ja *www.yksityisyydensuoja.fi* viittaavat samaan osoitteeseen. Jälkimmäisessä verkkoselain käyttää automaattisesti oletusarvoisia protokollia ja portteja (HTTP ja portti 80) sekä etsii palvelimelta oletuksena index.html-tiedoston. (Comer 2009, 54–55.)

Salaamaton yhteys alkaa URL-osoitteella *http://* ja salattu yhteys *https://*. Normaali HTTP-yhteys käyttää porttia 80 ja HTTPS-yhteys porttia 443. HTTPS-yhteyttä käytettäessä URL, dokumentin sisältö, selaimella täytetyt lomakkeet sekä palvelimelle lähetettävät evästeet salataan. (Stallings 2011, 506–507.)

HTTPS-tunnus verkkoselaimen osoitepalkissa www-sivun osoitteen alussa on merkkinä salatusta yhteydestä. Tämä tarkoittaa sitä, että esimerkiksi lomaketiedot tai sivuston kirjautumistiedot lähetetään palvelimelle salatun yhteyden läpi. Jos tieto ei ole salattu, liikkuu se selväkielisenä, jolloin ulkopuolinen hyökkääjä voi päästä siihen käsiksi. Tästä syystä asioimisessa verkkopankkien ja -kauppojen kanssa on olennaista tarkistaa, että salaus on päällä. Selaimen osoiterivillä näkyy HTTPS-tunnuksen lisäksi suljetun lukon kuva, kun salattu yhteys on muodostettu palvelimeen. Useissa selaimissa lukon kuvaketta klikkaamalla voi tarkastella tarkemmin SSL-varmennetta ja sen varmentajan tietoja.

4.4 DNS

DNS (Domain Name System) on Internetin nimipalvelujärjestelmä, joka muuntaa luettavat ja vertauskuvalliset nimet tietokoneosoitteiksi. Se koostuu useista järjestelmistä, joita kutsutaan nimipalvelimiksi. Nimipalvelujärjestelmää hyödyntävät monet sovellukset, kuten esimerkiksi verkkoselaimet ja

sähköpostisovellukset. Sovelluksesta tulee nimipalvelujärjestelmän asiakas silloin, kun se tarvitsee nimen muuntamista. Asiakkaana sovellus lähettää pyynnön nimipalvelimelle, joka etsii vastaavan osoitteen ja palauttaa sen. Jos nimipalvelin ei kykene vastaamaan pyyntöön, muuttuu itse nimipalvelin toisen nimipalvelimen asiakkaaksi, kunnes löytyy pyynnön palauttava palvelin. (Comer 2009, 69.) Jokainen DNS-tietokantaan tehty kirjaus sisältää kolme kohtaa: verkkotunnuksen eli domain-nimen, tietueen tyypin ja arvon. Tietueen tyyppi kertoo, miten arvo tulee tulkita. Se voi esimerkiksi ilmoittaa, että arvo tarkoittaa IP-osoitetta. (Comer 2009, 75.)

Verkkotunnukset ovat hierarkkisia siten, että tärkein osuus nimestä on oikealla. Muut vasemmalla puolella olevat segmentit määrittelevät puolestaan esimerkiksi organisaation yksittäisiä koneita. Nimipalvelujärjestelmä ei määrittele eri segmenttien määrää. Sen sijaan se määrittelee arvot tärkeimmille segmenteille, joita kutsutaan ylätason verkkotunnuksiksi (engl. *top-level domain, TLD*). Osa ylätason verkkotunnuksista on yleisluontoisia tunnuksia (engl. *Generic TLD*), mikä tarkoittaa, että ne ovat yleisesti käytettävissä olevia. Osa taas on rajattu erityisille ryhmille tai valtioille. Esimerkiksi *yksityisyydensuoja.info* on yleisluontoinen tunnus ja *yksityisyydensuoja.fi* on Suomen maatunnusta käyttävä verkkotunnus. Verkkotunnusten eteen laitettava www-tunnus tarkoittaa, että tunnuksen omaava tietokone jakaa dokumentteja HTTP-protokollalla eri asiakasohjelmille. Tunnus siis viittaa käytettävään palveluun ja on lähinnä ihmisiä helpottamaan laadittu käytäntö. (Comer 2009, 69–72.)

Nimipalvelinten merkitys korostuu verkkosivuja ylläpitäessä, mutta yksityisyyden suojan kannalta kotikäyttäjänkin on syytä ymmärtää niiden toiminta. Käyttöjärjestelmät nimittäin sisältävät nimipalvelun asiakasohjelmiston, joka aktivoituu verkko-osoitteita selvittäessä. Asiakasohjelmisto lähettää tällöin nimipalvelukyselyt eteenpäin automaattisesti haetulle tai manuaalisesti lisätylle nimipalvelimelle, joka tekee varsinaiset nimipalveluselvitykset. Normaalisti tällaisena nimipalvelimena toimii käyttäjän Internet-palveluntarjoajan oma nimipalvelin. (Viestintävirasto 2013.) Tämä merkitsee sitä, että operaattori näkee erikseen myös kaikki nimipalveluselvityspyynnöt, joista voidaan nähdä suoraan millä verkkosivuilla käyttäjä on käynyt.

DNS-asiakasohjelmiston nimipalvelimet voidaan asettaa ja vaihtaa joko reitittimen tai käyttöjärjestelmän verkkoyhteyden määrityksistä. Esimerkiksi Google tarjoaa omia nimipalvelimiaan 8.8.8.8 ja 8.8.4.4 (Google 2013) ja tietoturvayhtiö Comodo omiaan 8.26.56.26 ja 8.20.247.20 (Comodo 2013). Vaikka Googleen ei yksityisyyden kannalta ole järkevää luottaa (vrt. luku 6.4), on Googlen nimipalvelinten käytöllä kuitenkin omat hyvät puolensa. Ne ovat nopeita ja varsin laajalti käytössä olevia, mikä lisää yksityisyyden suojaa, koska tällöin yksittäisen käyttäjän jäljittäminen hankaloituu. Comodo puolestaan käyttää omia estolistojaan ja suodattaa haittaohjelmia sisältäviä verkkotunnuksia. Tämä lisää huomattavasti tietoturvallisuutta ja estää monia hyökkäyksiä www-sivuja selailtaessa. Nimipalveluiden vaihtamisen merkitys korostuu käytettäessä esimerkiksi VPN-ratkaisuja (vrt. luku 6.3).

Käyttöjärjestelmät käyttävät lisäksi hosts-nimistä tekstitiedostoa DNS-hakujensa tukena. DNS-asiakasohjelmat lukevat hosts-tiedoston sisällön käynnistyessään ja käyttävät sen merkintöjä hyödykseen. Kyseisen tiedoston avulla voidaan estää haluttujen verkkotunnuksien käyttö ohjaamalla ne reitittymään takaisin omaan koneeseen eli IP-osoitteeseen 127.0.0.1 (*localhost*). Windows-käyttöjärjestelmistä hosts-tiedosto löytyy tiedostojärjestelmän osoitteesta *%SystemRoot%\system32\drivers\etc\hosts*, Mac OS X -käyttöjärjestelmistä polusta */private/etc/hosts* ja Unixin kaltaisista käyttöjärjestelmistä polusta */etc/hosts*. Tiedostoon voisi lisätä esimerkiksi *127.0.0.1 yksityisyydensuoja.fi*, jolloin osoitteeseen menevät pyynnöt ohjautuisivat takaisin omaan koneeseen, eikä tällöin tietoja lähetettäisi kyseiseen osoitteeseen. Käytännössä tämä siis merkitsisi sitä, että yksityisyydensuoja.fi-verkkosivulle ei enää päästäisi. Tällä tavoin voitaisiin estää mm. kohdennettuja mainoksia tarjoavia tai haittaohjelmia levittäviä sivustoja.

Jos koneen nimipalvelimia tai hosts-tiedostoa muuttaa, niin on hyvä huomioida, etteivät muutokset tapahdu automaattisesti. Tällöin tietokoneen DNS-välimuisti pitää tyhjentää, tai yksinkertaisemmin käynnistää tietokone uudelleen. DNS-välimuistin tyhjennys onnistuu Windowsissa komentorivikehotteelta *ipconfig /flushdns* -komennolla. Tämän jälkeen DNS-palvelimien tiedot voidaan tarkistaa

esimerkiksi komennolla *nslookup yksityisyydensuoja.fi*. Vastaukseksi pitäisi saada tällöin muutetut palvelimet.

4.5 SSH

SSH (*Secure Shell*) on tietoturvallisuutta edistävä tietoliikenneprotokolla. Alkuperäinen versio SSH1 suunniteltiin pääteyhteyksien turvalliseen kirjautumiseen Internetissä. Sen tarkoitus oli korvata turvattomat ja salaamattomat etäyhteysprotokollat, kuten TELNET. SSH tarjoaa aiempia tekniikoita paremman asiakasohjelman ja palvelimen kyvykkyyden. Lisäksi sitä voidaan käyttää muihinkin verkkotoimintoihin, kuten tiedonsiirtoon ja sähköpostiviestintään. Protokollan uudempi versio SSH2 korjaa useita ensimmäisen version haavoittuvuuksia. (Stallings 2011, 508.)

SSH toimii sovelluskerroksessa ja sen avulla voidaan luoda ja käyttää turvallisempia etäyhteyksiä. Tyypillisesti SSH-protokollaa käytetään etäkoneisiin kirjautumiseen, mutta sillä voidaan toteuttaa myös mm. tunnelointiratkaisuja (vrt. luku 6.3) tai turvata tiedonsiirto. Kaupallista SSH-ohjelmistopakettia tarjoaa suomalainen SSH Communications Security (SSH Communications Security 2013), mutta tarjolla on myös vapaaseen lähdekoodiin perustuva OpenSSH. OpenSSH on ilmainen ja vaihtoehtoinen SSH-yhteystyökaluja tarjoava ohjelmistopaketti. Ohjelmistopaketti on ladattavissa ohjelman kotisivuilta osoitteesta http://www.openssh.com ja asennettavissa OpenBSD-käyttöjärjestelmälle (OpenSSH 2013).

Windows-käyttöjärjestelmässä SSH-palvelimen perustamisen ja SSH-yhteyden muodostamisen asiakasohjelmalla voi toteuttaa käyttämällä esimerkiksi Bitvisen kehittelemiä ohjelmia. Kyseisten ohjelmien avulla kotikäyttäjä voi luoda mm. tunneloinnin, turvallisen etäkäytön toiseen laitteeseen tai siirtää tiedostoja salatun yhteyden läpi. Henkilökohtaisessa ei-kaupallisessa tarkoituksessa ohjelmat ovat ilmaisia käyttää ja ne voidaan ladata yrityksen kotisivuilta osoitteesta https://www.bitvise.com. (Bitvise 2013.)

5 Anonyymit verkot

Anonyymeillä verkoilla tarkoitetaan verkkoja, jotka tarjoavat mahdollisuuden nimettömyyteen sekä pääsyn tietolähteisiin, joihin ei suoraan Internetistä käsin ole mahdollista päästä. Näihin verkkoihin viitataan toisinaan termillä *darknet*, mutta se saattaa harhaanjohtavasti sekoittua ns. ystäväverkkoihin (*F2F, Friend-to-friend*). F2F-ystäväverkot perustuvat anonymiteetin säilyttämiseen siten, että yhteydet muodostetaan vain luotettujen käyttäjien kanssa. Tällöin F2F-verkot eroavat perinteisemmistä vertaisverkoista (*P2P, peer-to-peer*) siten, etteivät käyttäjien IP-osoitteet ole julkisesti jaettavia, vaan ainoastaan näkyvissä luotetuille käyttäjille. Seuraavissa alaluvuissa käsitellään kolmea tunnetuinta anonymiteettiä tarjoavaa verkkoa ja niiden mahdollisuuksia yksityisyyden suojan parantamiseksi. Esitellyistä verkoista Freenet on toisaalta P2P- tai F2F-verkko, mutta tässä tutkielmassa viitataan selvyyden vuoksi kaikkiin esiteltyihin verkkoihin anonyymeillä verkoilla.

On syytä mainita, että tutkielmassa esiteltyjä verkkoja on laillista käyttää Suomessa, eikä niiden käyttäminen ole pätevä syy epäillä henkilöä rikoksesta. Esiteltyjä anonyymejä verkkoja ei ole myöskään tarkoitettu laittoman tai tekijänoikeuksia polkevan materiaalin julkaisemiseen ja lataamiseen, vaan niiden ensisijainen tehtävä on tarjota käyttäjilleen yksityisyyden suoja ja sananvapaus. Anonymiteetti ja sananvapaus kulkevat usein käsi kädessä, koska täydellistä sananvapautta ei voida taata ilman täydellistä anonymiteettiä ja sensuroimattomuutta. Anonyymejä verkkoja käytettäessä vastuu on aina käyttäjällä, kuten muuallakin Internetissä.

5.1 The Onion Router

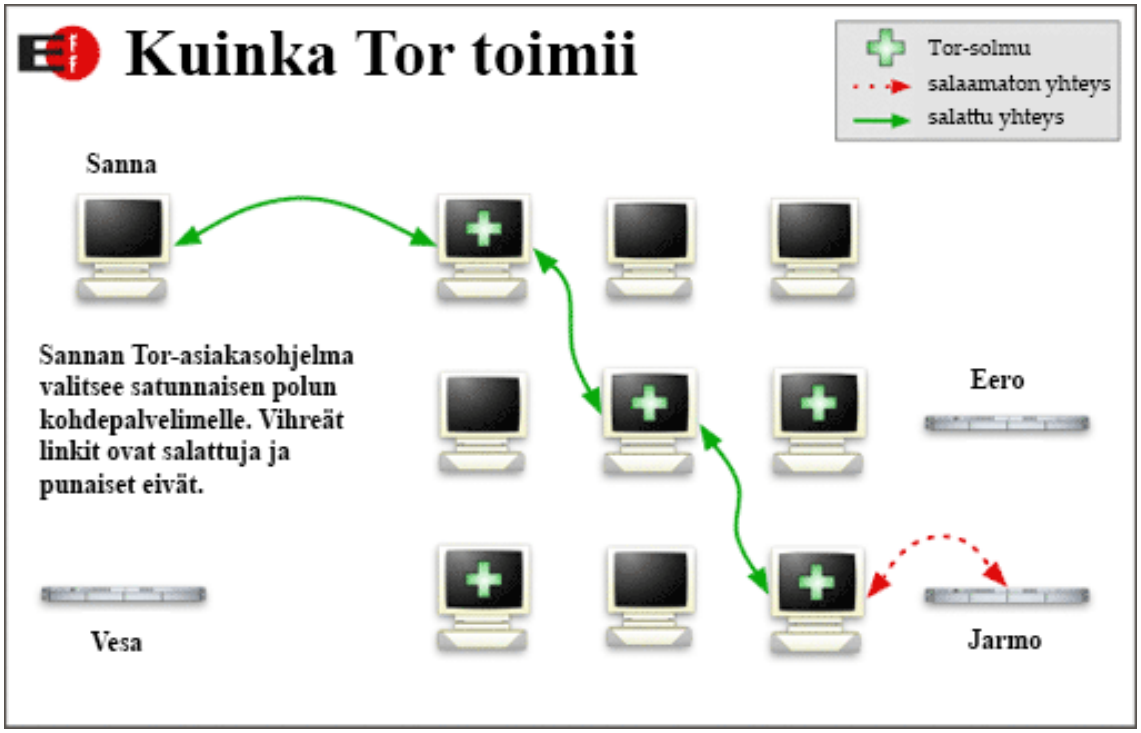
Sipulireititys eli Tor (*The Onion Router*) suunniteltiin ja kehitettiin alun perin Yhdysvaltain laivastolle. Sen ensisijaisena tarkoituksena oli suojella valtion viestintää. Nykyään sitä käyttävät mm. tavalliset ihmiset, toimittajat, lainvalvontaviranomaiset, armeijat sekä aktivistit useisiin eri tarkoituksiin.

Yksityishenkilöt käyttävät Tor-verkkoa estääkseen www-sivuja tarkkailemasta heitä, viestiäkseen anonyymisti tai kiertääkseen palveluntarjoajiensa asettamia sivustoestoja. Toimittajat käyttävät sitä keskustellakseen turvallisesti toisinajattelijoiden ja ilmiantajien kanssa. Kansalaisjärjestöt puolestaan hyödyntävät sitä antaakseen työntekijöillensä mahdollisuuden olla yhteydessä organisaatioonsa ilmoittamatta ulkopuolisille, että he työskentelevät kyseisessä organisaatiossa. Aktivistiryhmät, kuten Electronic Frontier Foundation (EFF), suosittelevat Tor-verkkoa keinona kansalaisoikeuksien säilyttämiseen tietoverkoissa. Yritykset käyttävät sitä kilpailukykyiseen analysointiin ja suojellakseen arkaluontoisia tietoja salakuuntelijoilta. Eräs Yhdysvaltojen laivaston osasto käyttää verkkoa julkisiin lähteisiin perustuvaan tiedusteluun, ja lainvalvojat käyttävät Tor-verkkoa verkkosivustojen valvontaan ilman, että jättävät hallitusten IP-osoitteita www-sivustojen verkkolokeihin. (The Tor Project 2013.)

Tor hajauttaa käyttäjän liikenteen useisiin eri paikkoihin Internetissä, jolloin mikään yksittäinen yhdistyspiste eli solmu ei voi assosioida käyttäjää määränpäähänsä. Sen sijaan, että otettaisiin Internet-verkon tapaan suora yhteys lähteestä määränpäähän, Tor-verkon datapaketit käyttävät satunnaista reittiä useiden eri palvelinten eli solmujen (engl. *node*) välityksellä. Palvelimet hävittävät jäljet siten, ettei mistään yksittäisestä reitityskohdasta voida kertoa, mistä paketti on tullut ja minne se on menossa. Asiakasohjelma neuvottelee jokaisen reitityspalvelimen kanssa erillisen salausavaimen varmistaakseen jäljittämättömyyden ja luo reitittimille ketjun. Kun reitittimien ketju on perustettu, voidaan tietoja vaihtaa ja sovelluksia käyttää Tor-verkon yli. Tehokkuuden saavuttamiseksi Tor käyttää samaa ketjua yhteyksille, jotka tapahtuvat kymmenen minuutin aikana. Myöhemmille pyynnöille rakennetaan uusi ketju, jottei aiempien toimintojen linkittäminen uudempiin onnistuisi. (The Tor Project 2013.)

Kuva 7 havainnollistaa Tor-verkon toimintaa. Sannan Tor-asiakasohjelman salaustavasta johtuen jokainen solmukohta ketjussa tietää vain viereisten solmujen IP-osoitteet. Esimerkiksi ensimmäinen solmukohta tietää, että Sannan asiakasohjelma lähetti sille jotain tietoa, jonka sen tulee lähettää seuraavalle

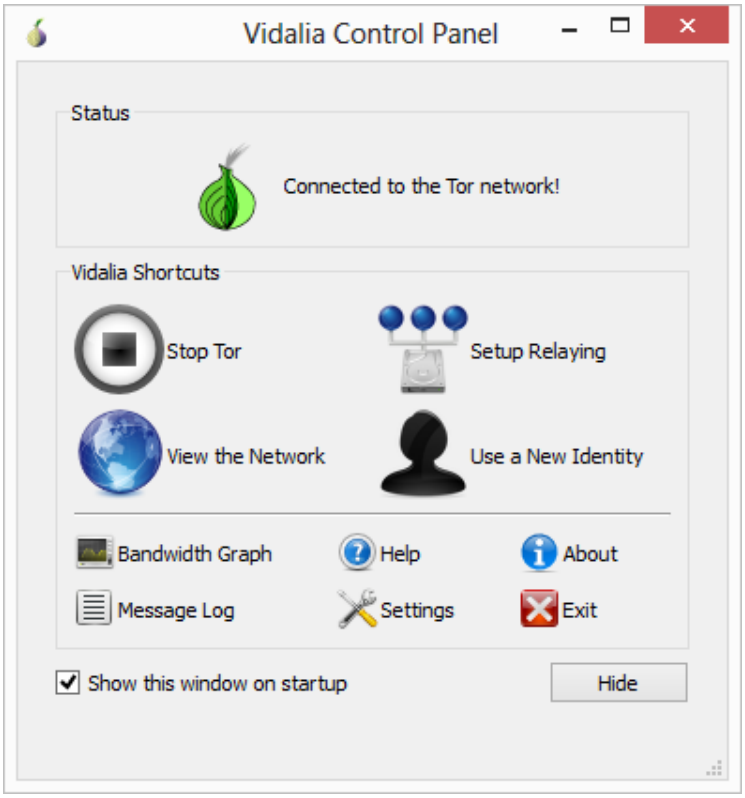
solmulle. Vastaavasti Jarmo tietää vain, että tiedot ovat tulleet viimeiseltä solmulta. Hänellä ei ole tietoa siitä, että Sanna lähetti tiedot. Reitityksessä tiedot liikkuvat salattuina, mutta lopuksi ketjun viimeinen solmu eli ulostulosolmu (engl. *exit node*) avaa salatun datan ja lähettää sen alkuperäisessä muodossaan kohdepalvelimelle. (Electronic Frontier Foundation 2013b.)



Kuva 7. Tor-verkon toimintaperiaate (The Tor Project 2013).

Tor tarjoaa mahdollisuuden käyttää sekä Internetiä että omassa verkossaan toimivia piilopalveluitaan (engl. *hidden service*) anonyymisti. Tor mahdollistaa käyttäjien sijainnin piilottamisen samalla, kun he tarjoavat erilaisia palveluita, kuten esimerkiksi verkkosivuja tai pikaviestintäpalvelimia. Tällöin muut käyttäjät voivat muodostaa yhteyden piilopalveluihin ilman, että kukaan tietää toisen verkkoidentiteettiä. Esimerkiksi piilopalvelu voisi sallia Tor-verkon käyttäjien perustaa verkkosivuja, jossa he voisivat julkaista aineistoa murehtimatta sensuurista. Nämä piilotetut palvelut toimivat omalla .onion-pseudoverkkotunnuksella. Sipulireitityksen .onion-tunnukset eivät ole varsinaisia DNS-nimiä (vrt. luku 4.4), vaan ne toimivat vain Tor-verkon välityspalvelinten avulla. (The Tor Project 2013.)

Tor-verkkoon pääsee helpoiten lataamalla Tor-projektin kotisivuilta TBB-selainpaketin (*Tor Browser Bundle*), joka sisältää Tor-verkkoa varten konfiguroidun TorBrowser-selaimen sekä Vidalia-ohjauspaneelin. Ohjelman voi ladata Windows-, Mac OS X- ja Linux-käyttöjärjestelmille osoitteesta https://www.torproject.org. Vidalia on graafinen ohjauspaneeli, joka avautuu ensimmäisenä TBB:n käynnistyessä (kuva 8). Sen avulla voidaan mm. käynnistää ja pysäyttää Tor, nähdä tietoja omasta kaistankäytöstä, vaihtaa identiteettiä, katsoa verkkolokitietoja sekä säätää asetuksia.



Kuva 8. Kuvakaappaus Vidalia-ohjauspaneelista yhdistettynä Tor-verkkoon (The Tor Project 2013).

Vidalia-ohjauspaneelin tila-kohdasta voidaan nähdä onko yhteys saavutettu. Tämän lisäksi TBB:n selain avaa oletuksena sivun *https://check.torproject.org*, joka tarkistaa onko yhteys Tor-verkkoon päällä ja mikä IP-osoite omalle yhteydelle on annettu. Tor-verkon piilopalveluita voi tämän jälkeen kokeilla esimerkiksi menemällä osoitteeseen *uptqndwzwrgm4juy.onion* (kuva 9). Kannattaa kuitenkin huomioida, että Tor-verkossa olevat piilopalvelut ovat yleensä saatavilla vain yhden sekä asiakasohjelmana että palvelimena toimivan tietokoneen ansiosta. Tämän takia sivustot ovat huomattavasti useammin

saavuttamattomissa kuin Internetissä toimivat www-verkkosivut. Ne siis eivät toimi silloin, kun niiden julkaisija tai julkaisun mahdollistava palvelu ei ole yhteydessä Tor-verkkoon.

Kuva 9. Kuvakaappaus Yksityisyydensuoja-sivustosta Tor-verkon osoitteessa uptqndwzwrgm4juy.onion. TorBrowser-selainohjelma sisältyy TBB-selainpakettiin (The Tor Project 2013).

Tor-verkon piilopalveluihin on mahdollista päästä myös Internetistä ilman Tor-asiakasohjelmaa käyttämällä Tor2web-palvelua. Kyseinen palvelu on tarkoitettu suojaamaan ainoastaan julkaisijat, mutta ei lukijoita. Siksi se ei tarjoa samanlaista anonymiteettiä, luottamuksellisuutta ja todennusta, jotka TBB mahdollistaa. Palvelua voi kokeilla Internetissä vaihtamalla selaimessa *.onion*-tunnus *.tor2web.org*-tunnukseen. (Tor2web 2013.) Esimerkiksi kuvassa 9 näkyvä osoite toimii Internetistä käsin syöttämällä osoite *https://uptqndwzwrgm4juy.tor2web.org* selaimelle. Muita Tor-verkon sivustoja voi etsiä esimerkiksi Ahmia.fi-palvelulla, joka löytyy osoitteesta *https://ahmia.fi/address* (Ahmia 2013).

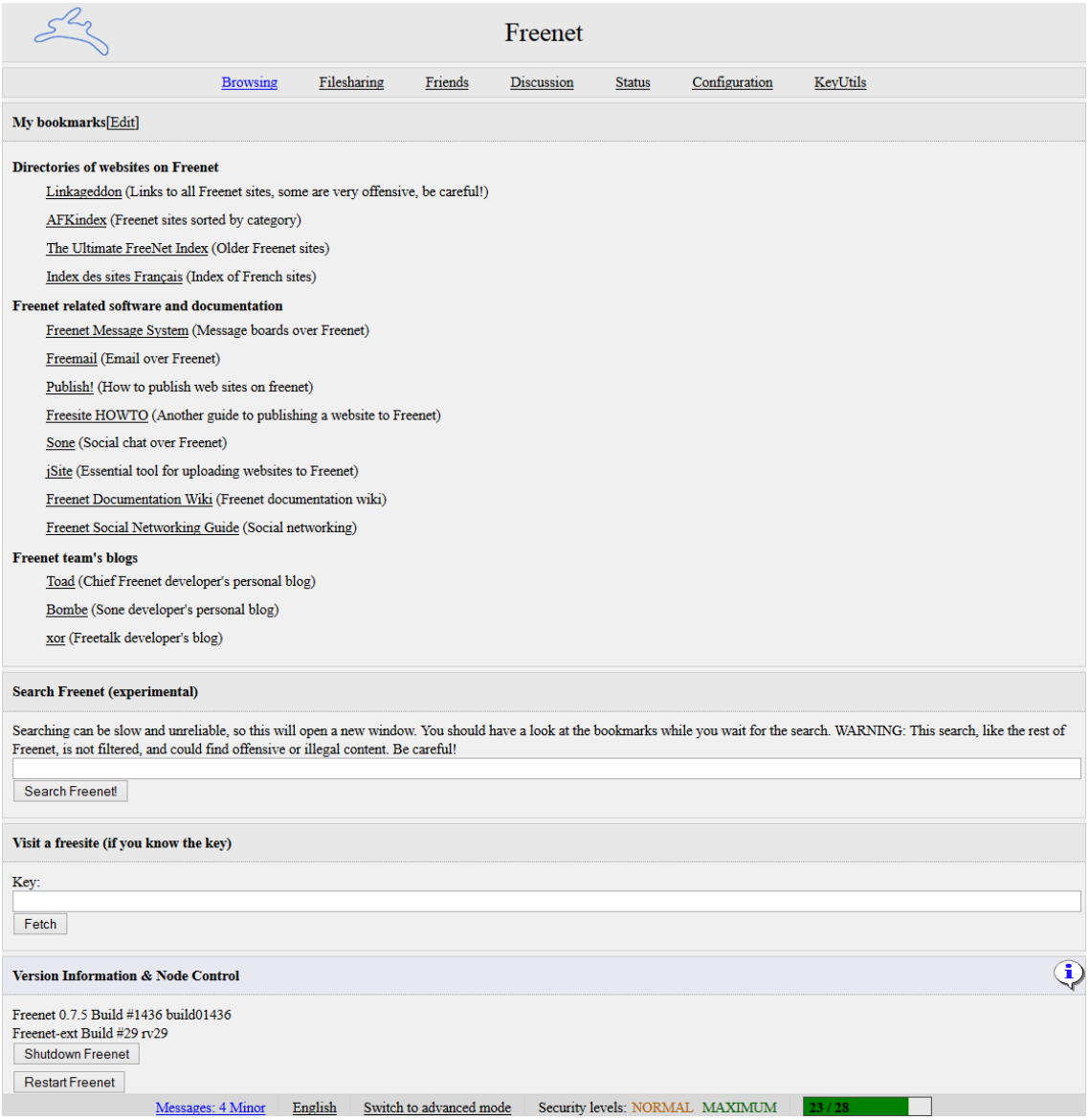
Helppokäyttöinen TBB-selainpaketti tarjoaa turvallisen, ilmaisen ja anonyymin tavan käyttää tietoverkkoja. Tor-verkko on eräs tärkeimmistä tavoista suojata Internetin käyttö tietoliikenteen tarkkailulta. Nopeudeltaan Tor häviää kuitenkin selkeästi maksullisille VPN-ratkaisuille (vrt. luku 6.3). Sen sijaan se tarjoaa ilmaiseksi anonyymiyden, mahdollisuuden tiedon sensuurittomaan julkaisemiseen sekä pääsyn sensuroimattomiin tietolähteisiin. Tor-verkkoa käytettäessä on kuitenkin hyvä pitää mielessä, että ulostulosolmusta voidaan nähdä verkossa liikkuva data samalla tavalla kuin Internet-palveluntarjoajakin voi nähdä sen ilman Tor-verkkoa. Kuka tahansa voi perustaa ulostulosolmun, ja onkin syytä huomioida, että niitä perustetaan myös tarkkailun mahdollistamiseksi. Tämän takia arkaluontoinen tieto on syytä salata myös Tor-verkkoa käytettäessä.

5.2 Freenet

Freenet on useista tietokoneista koostuva verkko, joka säilyttää ja noutaa tiedostoja. Verkkonsa avulla se tarjoaa mahdollisuuden viestiä turvallisesti ja yksityisyyden suojaa kunnioittavasti. Sen tarkoitus on taata kaikille anonyymiä ja sensuurista vapaata tiedonjulkaisemista. Freenet on myös ilmainen ohjelmisto, jonka käyttäminen on edellytys kyseiseen verkkoon liittymiselle. Se mahdollistaa anonyymin tiedostojen julkaisemisen ja lataamisen, verkon sisäisten sivujen (engl. *freesite*) selailun sekä niiden julkaisemisen. Freenetin sisäisille sivustoille on mahdollista päästä siis vain Freenetin kautta. (Freenet 2013.)

Freenetin solmujen (engl. *node*, vrt. luku 5.1) väliset yhteydet salataan ja reititetään muiden solmujen kautta, minkä vuoksi ulkopuolisen on äärimmäisen vaikea saada selville, kuka tietoa hakee ja mikä sen sisältö on. Käytön aikana käyttäjät lahjoittavat yhteisölle osan omasta datayhteydestään sekä kiintolevytilastaan. Verkon tiedot säilytetään ja tuhotaan sen perusteella, kuinka suosittuja ne ovat. Jokainen verkon käyttäjä sisällyttää osan tiedoista omalle koneelleen. Kiintolevylle tallennettavat tiedot kuitenkin salataan, jolloin käyttäjät eivät itse näe niiden sisältöä, eivätkä voi silloin olla vastuussa siitä. (Freenet 2013.)

Freenet-ohjelman voi ladata Windows-, Mac OS X- ja Linux-käyttöjärjestelmille osoitteesta https://freenetproject.org. Freenet on Java-ohjelma ja tarvitsee ajoaikaisen ympäristön toimiakseen (vrt. luku 3.2). Ohjelman asennusohjelmisto auttaa Javan asennuksessa, mikäli sitä ei ole ennestään asennettu. Tämän jälkeen valitaan hakemisto, johon Freenetin tiedot asennetaan. Tiedot voidaan halutessa asentaa myös salatulle osiolle (vrt. luku 3.4).



Kuva 10. Kuvakaappaus Freenetin aloitussivusta (Freenet 2013).

Asennuksen ja ohjelman avaamisen jälkeen Freenetin ohjattu asennustoiminto käynnistyy selaimeen, josta voidaan valita halutaanko käyttää opennet- vai darknet-tilaa. Opennet-tilassa käyttäjä yhdistetään kehen tahansa verkon käyttäjään, mikä on toiminnan kannalta ehdoton vaihtoehto, jos tiedossa ei ole

muita verkon käyttäjiä. Darknet-tilassa käyttäjä yhdistetään vain hänen luottamiinsa ystäviin, mikä takaa huomattavasti paremman anonymiteetin. Freenetin asennusohjelma tarjoaa myös kolmannen vaihtoehdon, jossa kokeneempi käyttäjä voi valita asetukset tarkemmin. Näitä asetuksia voidaan muuttaa jälkikäteen, joten yksinkertaisinta on valita aluksi opennet-tila. Tämän jälkeen valitaan verkosta tallennettavien tietojen tilan suuruus ja oma yhteysnopeus. Kun asennusohjelma on valmis, pääsee verkkoon menemällä yhdyskäytävänä toimivaan osoitteeseen http://127.0.0.1:portti. Freenet valitsee käyttämänsä portin satunnaisesti asennuksen yhteydessä, ja osoite 127.0.0.1 viittaa omaan koneeseen (vrt. luku 4.4). Kuvassa 10 näkyy Freenetin käynnistyessä avautuva aloitussivu, josta käsin voidaan säätää asetuksia ja siirtyä nopeasti eri palveluihin.

5.3 I2P

I2P (*The Invisible Internet Project*) on Javalla toteutettu, anonymiteetin mahdollistava verkko, jonka tarkoituksena on mahdollistaa turvallinen ja suojattu viestiminen. Kehitysprojekti alkoi vuonna 2003 ideasta kehittää Freenet-tietoverkkoa paremmaksi (vrt. edellinen luku). Tarkoituksena on rakentaa, kehittää ja ylläpitää tietoverkkoa, joka mahdollistaa turvallisen ja anonyymin kommunikoinnin. I2P tarjoaakin verkkoon kytkeytyneille tahoille mahdollisuuden kommunikoida anonyymisti siten, että sekä lähettäjä että vastaanottaja ovat tunnistamattomia sekä toisillensa että kolmansille osapuolille. (I2P 2013.)

I2P rakentaa Tor-verkon tavoin tietoliikenneverkkoon oman kerroksen, joka mahdollistaa henkilöllisyyttä suojaavien sovellusten lähettää viestejä toisilleen turvallisesti ja anonyymisti. Kaikki lähetettävät tiedot kääritään neljän salauksen mahdollistavan kerroksen taakse. Kullakin asiakasohjelmalla on viestinnän salaamiseen oma I2P-reitityksensä, joka koostuu sekä lähettäjälle tulevista että lähettäjältä lähtevistä tunneleista. Tunnelilla tarkoitetaan I2P-reitittimien läpi ohjattua polkua ja niiden avulla viestejä voidaan lähettää vain yhteen suuntaan. Kun viesti halutaan lähettää takaisin, tarvitaan sitä varten toinen tunneli. (I2P 2013.)

I2P-verkossa on mahdollista julkaista anonyymisti myös vain kyseisessä verkossa toimivia verkkosivuja (*eepsite*). Nämä sivustot toimivat päätteellä .i2p. Tämän lisäksi verkossa on mahdollista julkaista monia muita interaktiivisia verkkopalveluita Tor-verkon tavoin. I2P eroaa Tor-verkosta mm. siten, että sitä vastaan ei ole asetettu valtioiden ja operaattorien taholta niin paljon estoja kuin Tor-verkolle. Lisäksi rakennetut tunnelit ovat lyhytikäisempiä kuin Tor-verkon ketjut ja sen piilotetut palvelut toimivat usein nopeammin. Sekä Tor että I2P eroavat Freenetistä tarjoamalla interaktiivista sisältöä, kun taas Freenet on enemmänkin anonyymi julkaisualusta. (I2P 2013.)

I2P-ohjelman voi ladata Windows-, Mac OS X- ja Linux-käyttöjärjestelmille osoitteesta http://www.i2p2.de. Freenetin tavoin I2P vaatii Javan ajoaikaisen ympäristön toimiakseen. Asentamisen ja I2P-reitityksen käynnistämisen jälkeen avautuu aloitusvalikko, josta voidaan nopeasti päästä useisiin oleellisiin palveluihin (kuva 11).

Kuva 11. Kuvakaappaus I2P:n aloitussivusta Iceweasel-selaimesta käsin (I2P 2013).

Anonyymit verkot tarjoavat tehokkaita keinoja yksityisyyden suojan parantamiseen esimerkiksi suojaamalla käyttäjän IP-osoitteen, tarjoamalla suojatumman alustan sähköpostiviestien säilyttämiseen, lähettämiseen ja lukemiseen sekä mahdollistamalla yksityisen ja tarvittaessa anonyymin pikaviestinnän. Anonyymejä verkkoja käytettäessä on kuitenkin hyvä tiedostaa, että itse verkon käyttäminen ei yleensä ole salattua tietoa. Esimerkiksi Internet-palveluntarjoaja voi nähdä, kun verkkoja hyödynnetään. Suomessa asialla ei pitäisi olla suurta merkitystä, koska verkkojen käyttäminen on laillista, eikä myöskään Internet-palveluntarjoajien sensuurin alaista. Verkkojen käyttöä on mahdollista kuitenkin peitellä esimerkiksi hyödyntämällä VPN-palveluita, joista kerrotaan tarkemmin luvussa 6.3. Tällöin yhteys muodostetaan ensin VPN-palvelun kautta ja vasta sen jälkeen anonyymiin verkkoon.

6 Suojattu viestintä

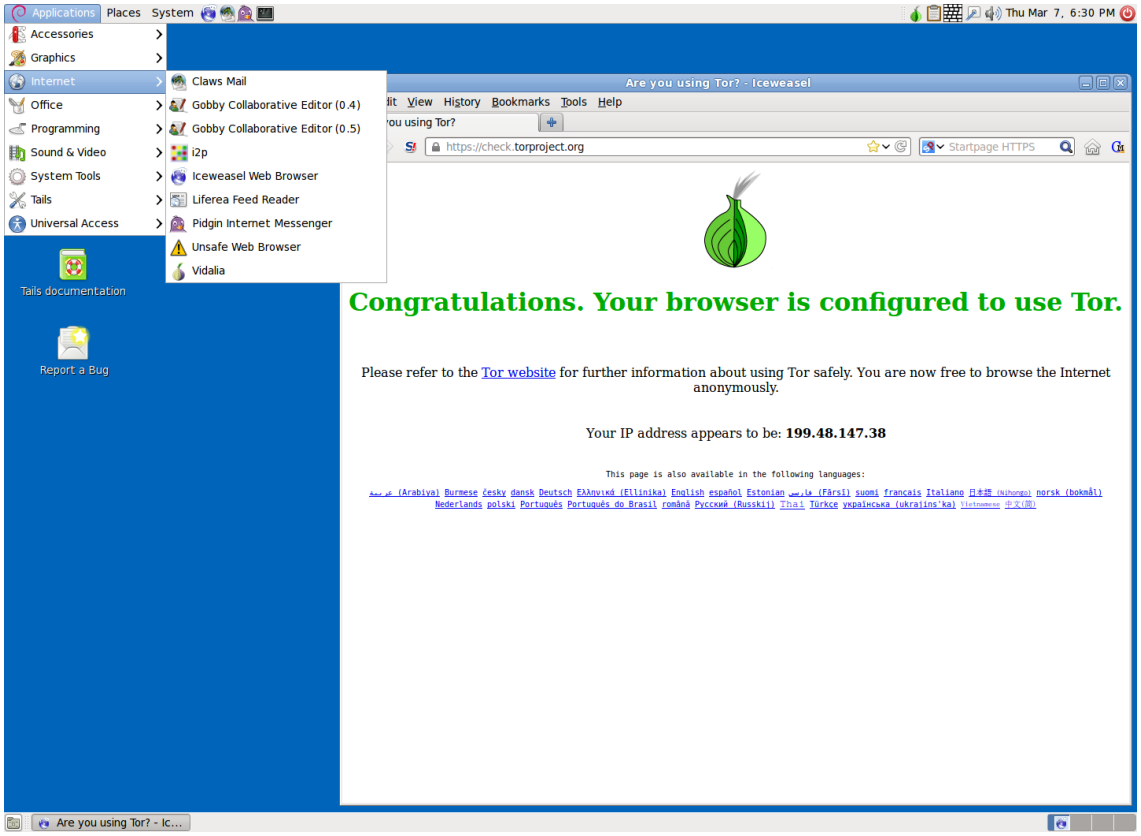
Tämän luvun tarkoituksena on kuvata keinoja, joilla Internetissä tapahtuvaa viestintää voitaisiin suojata tehokkaammin. Esitellyt menetelmät ja seikat hyödyntävät osittain aiemmin selvitettyjä protokollia ja asioita. Ensin kerrotaan erityisistä käyttöjärjestelmistä, jotka tukevat useita eri salausmenetelmiä ja antavat nopeasti tehokkaan suojan käyttäjälle. Tämän jälkeen siirrytään oman IP-osoitteen suojaamiseen välityspalvelinten ja VPN-palveluiden avulla sekä hakukoneiden anonyymiin käyttöön. Lopuksi kerrotaan metatiedon merkityksestä ja sen poistamisesta sekä sähköposti- ja pikaviestinnän suojauksesta.

6.1 Identiteettiä suojaavat käyttöjärjestelmät

Yksityisyyden suojan ja anonymiteetin parantamista varten on kehitetty erityisiä käyttöjärjestelmiä, jotka pyrkivät automaattisesti varmistamaan käyttäjän anonymiteetin ja tietoturvan. Näistä kuuluisimmat ovat Debian GNU/Linux -jakeluun perustuva Tails ja Gentoo GNU/Linux -jakeluun perustuva Liberté Linux. Molemmat on tarkoitettu käytettäväksi suoraan cd-levyltä, dvd-levyltä tai

muistitikulta, jolloin käyttäjän toimet eivät jätä käytettävän tietokoneen kiintolevyille mitään tietoja. Näiden lisäksi on olemassa huomionarvoinen virtualisointiin perustuva Whonix-käyttöjärjestelmä.

Tails käyttää Tor-verkkoa säilyttääkseen käyttäjän yksityisyyden suojan Internetissä (kuva 12). Kaikki suorat verkkoyhteydet on torjuttu, ja verkkoyhteyttä käyttävät ohjelmat on automaattisesti asetettu yhdistymään Tor-verkon kautta. Tor-verkon lisäksi Tails kykenee yhdistämään käyttäjän I2P-verkkoon. Tiedon tallentamiseen Tails hyödyntää ainoastaan tietokoneen keskusmuistia, joka pyyhitään automaattisesti koneen sulkemisen yhteydessä. Tällöin käytöstä ei jää jälkiä hyödynnettyyn tietokoneeseen. Tiedostoja voi kuitenkin tallentaa erilliselle muistitikulle tai ulkoiselle kiintolevylle. (Tails 2013.)



Kuva 12. Kuvakaappaus Tails-käyttöjärjestelmän graafisesta käyttöliittymästä (Tails 2013).

Tails sisältää myös useita valmiiksi asennettuja työkaluja käyttäjän yksityisyyden suojan parantamiseksi. Näitä ovat mm. LUKS-työkalu muistitikkujen ja ulkoisten kiintolevyjen salausta varten (vrt. luku 3.4), virtuaalinen näppäimistö näppäilyn

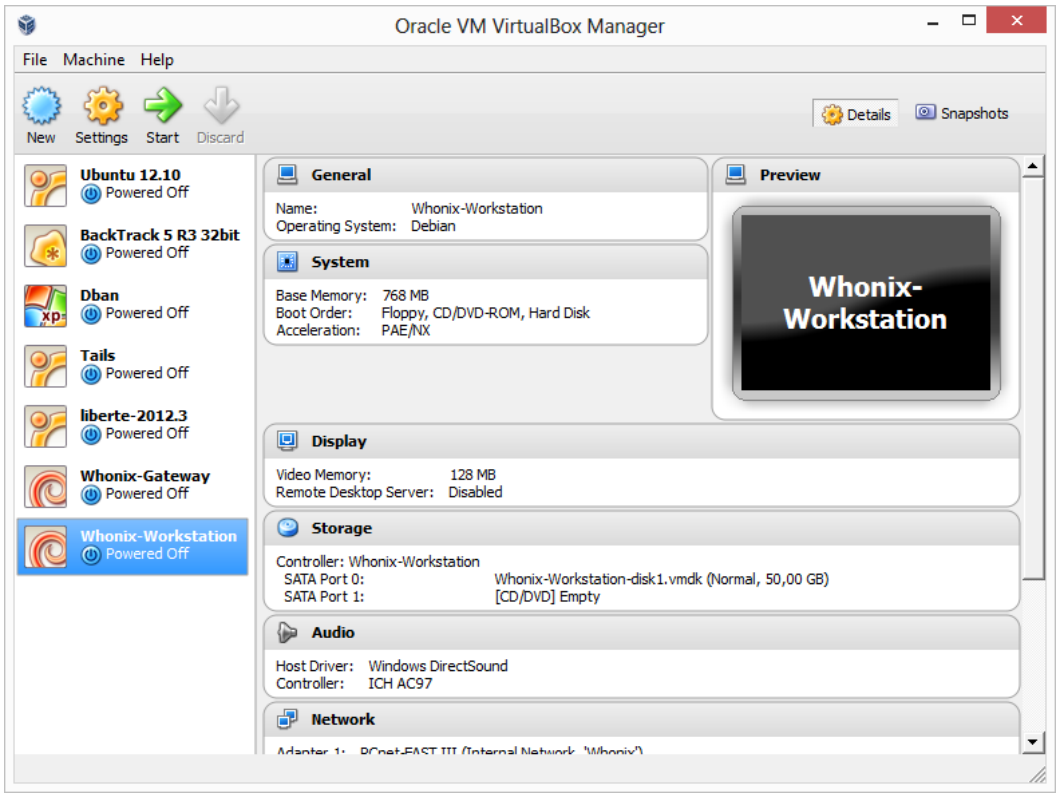
tallentajien estämiseksi (vrt. luku 3.3), OpenPGP-työkalut sähköpostien salaamista varten (vrt. luku 6.6.1), HTTPS Everywhere -selainlaajennus (vrt. luku 3.2), KeePassX-salasananhallintaohjelma (vrt. luku 3.3), metatiedon poistamistyökalu (vrt. luku 6.5), OTR-työkalu pikaviestinnän salaukseen (vrt. luku 6.7) sekä Nautilus Wipe -työkalu turvalliseen tietojen hävittämiseen (vrt. luku 3.5). Näiden lisäksi käyttöjärjestelmään on asennettu mm. verkkoselain, pikaviestintäohjelma, sähköpostiohjelma, OpenOffice-paketti sekä kuvan ja äänen muokkaamisohjelma. Tailsin voi ladata ilmaiseksi ohjelman kotisivuilta osoitteesta https://tails.boum.org. (Tails 2013.)

Myös Liberté Linux on turvallinen ja anonyymi käyttöjärjestelmä, jonka ensisijainen tarkoitus on tarjota luotettava ja salattu kommunikointimahdollisuus vihamielisessä ympäristössä (kuva 13). Tailsin tavoin kaikki verkkoliikenne kulkee Tor-verkon läpi. Käyttöjärjestelmä mahdollistaa I2P:n käytön, mutta sekin liikenne kulkeutuu Tor-verkon kautta. Libertén asennus vie tilaa vain noin 210 megatavua, ja toimiakseen käyttöjärjestelmä vaatii koneelta vain 192 megatavua keskusmuistia. (Liberté Linux 2012.)

Kuva 13. Kuvakaappaus Liberté Linux -käyttöjärjestelmän graafisesta käyttöliittymästä. Käyttöjärjestelmän on kehittänyt Maxim Kammerer (Liberté Linux 2012).

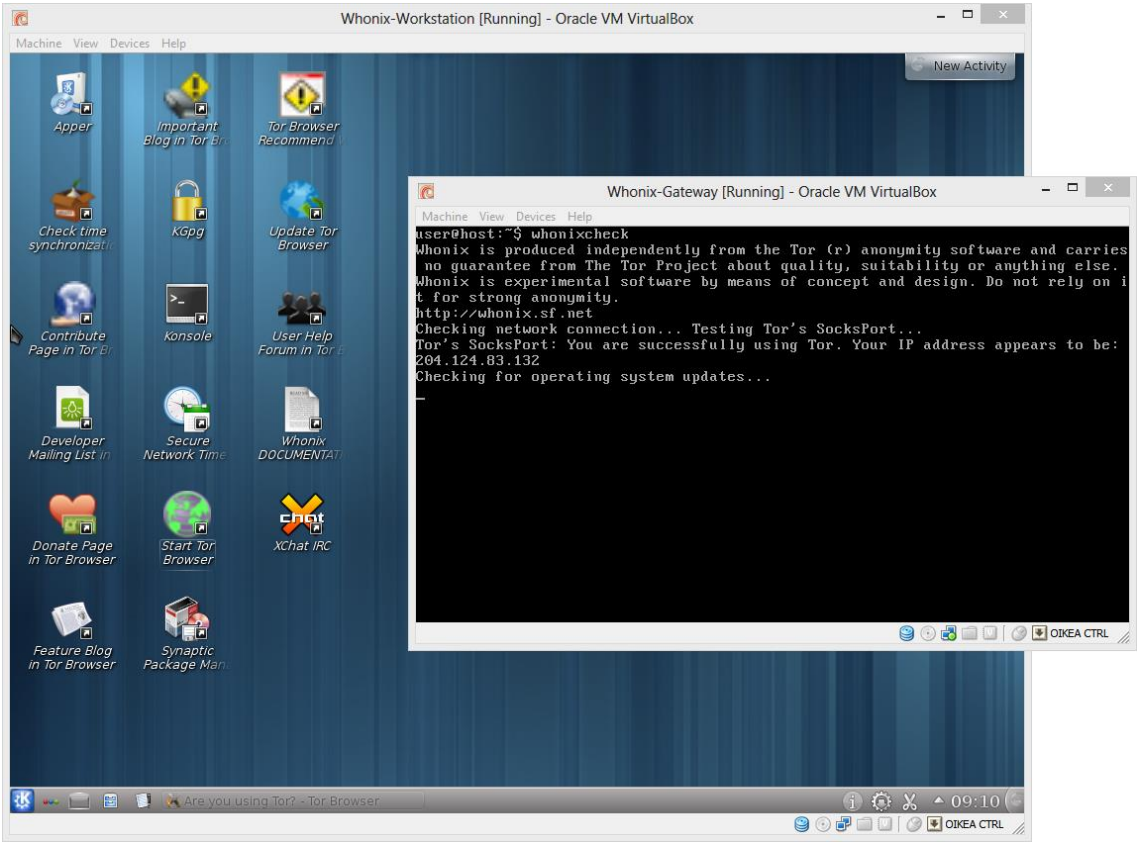
Libertén kaikki asetukset ovat valmiiksi konfiguroituja yksityisyyden suojaa ajatellen. Ainoa toimenpide, joka käyttäjältä vaaditaan käynnistyksen yhteydessä, on suojatun osion salasanan luonti. Säilytykseen jäävien tietojen salaukseen käytetään Tailsin tavoin LUKS-työkalua. Liberté ei myöskään jätä käytettyyn tietokoneeseen jälkiä, ellei käyttäjä itse päätä niin tehdä esimerkiksi kopioimalla jotain kiintolevyille. Yksityisyyden suojaa parannetaan myös muuttamalla langattomien verkkosovittimien MAC-osoitteita (*Media Acccess Control*) automaattisesti, jotta niiden jäljittäminen hankaloituisi. Verkkokortin valmistamisen yhteydessä luotu MAC-osoite yksilöi verkkosovittimen, mutta sen muuttaminen on mahdollista ohjelmallisesti. Liberté Linux on ilmainen ohjelma ja sen voi ladata osoitteesta http://dee.su/liberte. (Liberté Linux 2012.)

Whonix on Debian GNU/Linux -käyttöjärjestelmä, joka hyödyntää toiminnassaan virtuaalikoneita ja Tor-verkkoa. Virtuaalikone on ympäristö, jossa voidaan tietokoneen tavoin suorittaa ohjelmia. Esimerkiksi Oraclen avoimeen lähdekoodiin perustuva VirtualBox-virtualisointiohjelmisto mahdollistaa virtuaalikoneiden suorittamisen Windows-, Mac OS X- ja Linux-käyttöjärjestelmissä. Se tarjoaa virtuaalisen järjestelmäalustan, jolloin varsinaisen käyttöjärjestelmän sisältä voidaan suorittaa muita käyttöjärjestelmiä. VirtualBoxin voi ladata ohjelman kotisivuilta osoitteesta https://www.virtualbox.org. (VirtualBox 2013.) Kuvassa 14 on VirtualBox-ohjelma omassa pääikkunassaan.



Kuva 14. Kuvakaappaus Oracle VirtualBox -virtualisointiohjelmasta (VirtualBox 2013).

Whonix koostuu kahdesta erillisestä virtuaalikoneesta, joita voidaan käyttää VirtualBoxista käsin. Whonix-Gateway toimii yhdyskäytävänä Tor-verkkoon ja Whonix-Workstation toimii graafisena käyttöjärjestelmänä sekä eristettynä verkkona. Kaikki Whonix-Workstationin verkkoyhteydet on pakotettu menemään yhdyskäytävän läpi, mikä reitittää yhteydet Tor-verkon kautta. Tällöin IP- ja DNS-vuodot (vrt. luvut 4.4 ja 6.3) ovat mahdottomia, eivätkä edes järjestelmänvalvojan oikeuksilla toimivat haittaohjelmat voi saada selville käyttäjän todellista IP-osoitetta. (Whonix 2013.) Kuvassa 15 ovat Whonix-Gateway ja Whonix-Workstation käynnistettyinä omiin virtuaalikoneisiinsa.



Kuva 15. Kuvakaappaus Whonix-käyttöjärjestelmästä VirtualBoxin virtuaalikoneina (Whonix 2013, VirtualBox 2013).

Whonix tarjoaa Tailsin ja Libertén tavoin useita valmiiksi asennettuja ohjelmia yksityisyyden suojan lisäämiseen. Näitä ovat mm. käyttöliittymä GnuPG-salaustyökaluille (vrt. luku 6.6.1), metatiedon poistotyökalu (vrt. luku 6.5) ja virtuaalinen näppäimistö (vrt. luku 3.3). Whonixin voi ladata ilmaiseksi sen kotisivuilta osoitteesta http://sourceforge.net/p/whonix.

6.2 Välityspalvelimet

Välityspalvelin (engl. *proxy server*) tarkoittaa palvelinta, joka reitittää yhteyden käytettävän laitteen ja kohdepalvelimen välillä. Kun esimerkiksi verkkoselain on asetettu käyttämään välityspalvelinta, se tekee kaikki pyynnöt kyseiselle palvelimelle. Välityspalvelin välittää pyynnöt eteenpäin halutuille palvelimille ja palauttaa vastaukset takaisin selaimelle. (Stuttard & Pinto 2011, 49–50.) Välityspalvelin ei kuitenkaan tarjoa kunnollista anonymiteettiä, koska palvelin voi kaapata kaiken sen läpi kulkevan liikenteen. Julkisesti käytettävien

välityspalvelinten käyttäminen on yksityisyyden suojan kannalta vaarallista myös sen takia, että ne ovat hyvin alttiita ulkopuolisille verkkohyökkäyksille. Tämän vuoksi yhteen välityspalvelimeen muodostettua yhteyttä voidaankin ajatella lähinnä satunnaisen, maakohtaisen sensuroinnin kiertämiseen tai oman IP-osoitteen piilottamiseen vierailtavalta verkkosivulta. Välityspalvelimen toimintaa voidaan kokeilla esimerkiksi webkäyttöliittymällä toimivalla palvelulla. Tällainen on mm. SSL Proxy, joka hyödyntää Glypen tarjoamaa ohjelmakoodia (Glype 2013). Ilmaista palvelua voi käyttää osoitteessa *https://www.proxyssl.org*, mutta kannattaa muistaa, että sekään ei tarjoa kunnollista suojaa (SSL Proxy 2013).

Perinteistä yhden välityspalvelimen kautta yhdistävää tekniikkaa kehittyneempi toteutustapa on useiden välityspalvelinten kautta yhdistävä palvelu. Selvyyden vuoksi tässä tutkielmassa se suomennetaan sekoiteverkoksi (engl. *Mix Cascade*, *Mix Network*). Sekoiteverkossa verkkoyhteys yhdistetään useiden välikäsien eli sekoitteiden (engl. *mixes*) kautta. Käytännössä tämä tarkoittaa sitä, että käyttäjä yhdistyy usean eri välityspalvelimena toimivan sekoitteen kautta, jolloin käyttäjän todellinen IP-osoite onnistutaan salaamaan tehokkaammin (JAP Anonymity & Privacy 2013). Esimerkiksi aiemmin esitellyt sipulireititys ja I2P-tekniikat ovat eräänlaisia sekoiteverkkoja (vrt. luku 5.1).

Kaupallista sekoiteverkkoa tarjoaa JonDonym, joka on jatkokehitelty AN.ON-projektista (*Anonymity.Online*). JonDo on asiakasohjelma eli välityspalvelinohjelmisto, joka yhdistää käyttäjät JonDonym/AN.ON-sekoiteverkkoon. Verkossa liikkuva data salataan useaan kertaan, koska jokainen sekoiteverkossa toimiva palvelin salaa liikenteen erikseen (kuva 16). Tämän vuoksi Internet-palveluntarjoaja tai samassa langattomassa verkossa oleva hyökkääjä ei voi saada selville, millä verkkosivuilla palvelua käyttävä vierailee. (JonDonym 2013b.)

Kuva 16. Kaupallisen JonDonym sekoiteverkon toiminta (JonDonym 2013b).

JonDonym-verkossa hallitusten tai lainvalvontaviranomaisten on mahdollista tarkkailla tietoliikennettä, mutta vain silloin, kun heillä on oikeuden määräys tarkkailulle jokaiseen sekoitteessa toimivaan palvelimeen. Normaalisti JonDonym-sekoitteet eivät kerää lokitietoja verkossa liikkuvasta datasta, mutta oikeuden määräyksestä tämä on kuitenkin mahdollista. On myös syytä huomioida, että vain JonDo-ohjelmistoa käyttämään konfiguroidut ohjelmistot tarjoavat suojatun verkkoyhteyden. JonDonym-palveluun voi tutustua sen kotisivuilla osoitteessa *https://anonymous-proxy-servers.net*, ja maksullista palvelua voi kokeilla myös ilmaiseksi. Varsinaista JonDo-ohjelmistoa on mahdollista käyttää ilmaiseksi, mutta silloin se tarjoaa vain rajoitetun määrän sekoitteita ja hitaamman yhteysnopeuden. (JonDonym 2013a.) Tämän lisäksi sivuilta voidaan ladata Debian GNU/Linuxiin pohjautuvan JonDo-käyttöjärjestelmä, joka on hieman samankaltainen kuin edellisessä luvussa esitellyt Tails ja Liberté Linux. Käyttöjärjestelmä tukee mm. JonDonym-palvelua ja Tor-verkkoa.

6.3 VPN

VPN (*Virtual Private Network*) eli virtuaalinen erillisverkko on yksi käytetyimmistä salausta tarjoavista suojaustekniikoista, jotka mahdollistavat turvallisen pääsyn organisaation lähiverkkoon eli intranettiin. Teknologia suunniteltiin alun perin edulliseksi ratkaisuksi yhdistämään verkon välityksellä useita, maantieteellisesti hajautettuja organisaatioiden toimipaikkoja. Nykyisin VPN-yhteyksiä hyödynnetään myös yksityishenkilöiden verkkoviestinnän suojelemiseen ja anonymiteetin saavuttamiseen. VPN-ohjelmisto salaa ja purkaa datapaketteja ja lähettää ne tunneloinnin läpi. Kuten konkreettisessa tunnelissa kulkevat autot ja junat, data ei voi siirtyä muualle kuin tunnelin toiseen päähän. (Feilner 2006, 6, 12.)

VPN-yhteyttä tukevia protokollia on useita ja ne voidaan luokitella esimerkiksi TCP/IP-viitemallien kerroksien mukaan (vrt. luku 4.1). Siirtoyhteyskerrosta hyödyntävien menetelmien merkittävä etu on, että ne voivat siirtää muitakin kuin vain IP-protokollia. Näistä tunnetuimmat, salausta ja todennusta käyttävät protokollat ovat PPTP, L2F, L2TP ja L2Sec. PPTP (*Point-to-Point Tunneling Protocol*) kehiteltiin Microsoftin avulla PPP-protokollan laajennukseksi. Se on integroituna uudemmissa Windows-käyttöjärjestelmissä ja mahdollistaa niistä käsin helppokäyttöisen yhteyden muodostamisen. L2F (*Layer 2 Forwarding*) on lähinnä Ciscon kehittämä protokolla, joka tarjoaa hieman enemmän mahdollisuuksia kuin PPTP, mm. useiden samanaikaisten yhteyksien tunneloinnin. L2TP (*Layer 2 Tunneling Protocol*) on hyväksytty alan standardiksi ja sitä käytetään laajalti. Se yhdistää PPTP- ja L2F-protokollien vahvuudet, mutta ei kärsi näiden heikkouksista. L2TP voidaan yhdistää muihin teknologioihin, jotka tarjoavat erilaisia mekanismeja, kuten IPsec-prokollan. L2Sec (*Layer 2 Security Protocol*) luotiin ratkaisemaan IPsec-protokollan hyödyntämisessä esiintyvät turvallisuuspuutteet. Sen turvallisuusmekanismit ovat tehokkaampia, koska siinä käytetään pääosin SSL/TLS salausta. (Feilner 2006, 13–14.)

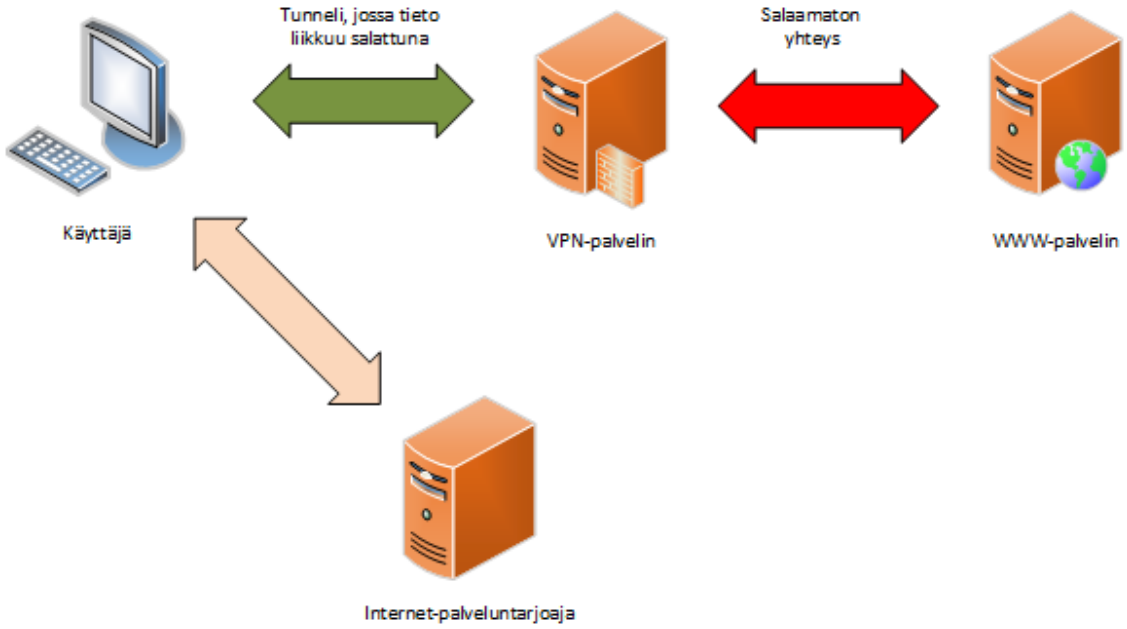
IPsec on todennäköisesti levinnein tunnelointiteknologia. Verkkokerroksella toteutettava IPsec on todellisuudessa enemmänkin protokollien ja mekanismien kokoelma kuin yksi teknologia. Suurin etu on sen laajalle levinnyt käyttö, mutta

haittapuolena on monimutkainen teknologia useiden erilaisten toteutusten ja porsaanreikien vuoksi. (Feilner 2006, 14.)

VPN-tunnelointi on mahdollista toteuttaa myös pelkästään sovelluskerroksessa. Käyttäjä voi päästä yrityksen VPN-verkkoon verkkoselaimellaan pelkästään kirjautumalla HTTPS-protokollalla suojattuun sivustoon. Tällöin tietoturva saavutetaan salaamalla liikenne käyttämällä SSL/TSL-tekniikkaa (vrt. luku 4.2). (Feilner 2006, 15.)

OpenVPN on merkittävä VPN-ratkaisu, joka perustuu vapaaseen lähdekoodiin ja on edellä esiteltyjä toteutuksia uudempi. Se toteuttaa verkkokerroksen tai siirtokerroksen yhteydet, käyttää SSL/TLS-protokollia salaukseen sekä yhdistää lähes kaikki aiemmin mainittujen ratkaisujen ominaisuudet. (Feilner 2006, 15.) Tämän vuoksi OpenVPN on vaihtoehtona suositeltavin VPN-ratkaisu.

Yksityisyyden suojan näkökulmasta VPN-yhteyksiä voidaan käyttää salaamaan oma Internet-liikenne mm. Internet-palveluntarjoajien tarkkailulta (engl. *Internet Service Provider, ISP*), verkkosivujen tarkkailulta sekä ohittamaan verkkopalveluille asetetut maantieteelliset estot. VPN-yhteyden muodostamisen jälkeen data liikkuu salattuna Internetissä, jolloin ulkopuolinen ei pääse tietoihin käsiksi. Vaikka verkossa liikkuvat datapaketit onnistuttaisiin kaappaamaan, eivät ne paljasta tietojaan kaappaajalle salauksen ansiosta. VPN-palvelut ovatkin yksityisyyden suojan kannalta eräs tärkeimmistä keinoista suojata oma Internet-liikenne ulkopuoliselta tarkkailulta. Internet-palveluntarjoaja näkee vain sen, että yhteys muodostetaan VPN-palvelimeen, muttei salauksen ansiosta näe palvelun kautta käytettävää dataa (kuva 17). Yhtälailla verkkosivut näkevät vain sen, että VPN-palvelusta muodostetaan yhteys, mutta ne eivät näe käyttäjän todellista IP-osoitetta.



Kuva 17. VPN-palvelun toimintaperiaate.

VPN-palvelua käytettäessä on tärkeä huomioida, että kaiken liikenteen on syytä kulkea palvelun kautta. Mikäli osa liikenteestä liikkuu salaamattomana, altistuu muukin liikenne tarkkailulle. Eräs suurimmista uhkista tällaiselle on DNS-vuoto. Vaikka VPN-yhteys olisikin muodostettu, käyttöjärjestelmä saattaa tietyissä olosuhteissa käyttää oletuksena olevia nimipalvelimia (vrt. luku 4.4). Tällöin nimipalvelimien pyyntötiedot saattavat vuotaa Internet-palveluntarjoajalle, ja käyttäjälle voi jäädä valheellinen turvallisuudentunne omasta yksityisyydestään. Osa VPN-palveluista tarjoaa DNS-vuotoja varten myös omia nimipalvelimia ja suojausmahdollisuuksia, joita on suositeltavaa käyttää. Vuotoja voidaan estää myös estämällä ne palomuurista käsin.

Anonymiteetin mahdollistavia VPN-palveluita tarjoavia yrityksiä on runsaasti, mutta suurimpana ongelmana palvelun valinnassa on luottamus. VPN-palvelun käyttäminen ratkaisee luottamuspulan oman Internet-palveluntarjoajan suhteen, koska se peittää käyttäjän lähettämän ja vastaanottaman datan. VPN-yhteyden tarjoaja näkee kuitenkin käytettävän liikenteen ja voi raportoida sen lokitietoihinsa ja myöhemmin jakaa nämä tiedot kolmansille osapuolille. Esimerkiksi englantilainen HideMyAss-niminen VPN-palveluntarjoaja nousi kyseenalaiseen julkisuuteen vuodettuaan FBI:lle LulzSec-hakkeriryhmään kuuluvan henkilön tiedot (Jowitt 2011). Tämän vuoksi VPN-palveluntarjoajien tietosuojaehtoihin on

syytä perehtyä tarkkaan. Osa palveluista ilmoittaa, etteivät ne säilytä lokitietoja palvelintensa kautta kulkevasta verkkoliikenteestä tai käyttäjiä identifioivista tiedoista. Käytännössä käyttäjä joutuu luottamaan palveluntarjoajan ilmoittamiin tietoihin, jotka saattavat kuitenkin nopeasti muuttua, jos palveluntarjoajia aletaan painostamaan oikeuskanteilla.

Yleisesti ottaen voidaan todeta, että ilmaiset VPN-palvelut eivät ole järkevä vaihtoehto. Ilmaisissa palveluissa käyttäjän verkkoliikenne saatetaan myydä eteenpäin esimerkiksi kaupallisiin tarkoituksiin. Liikenne ei myöskään ole usein tehokkaasti salattua ja se voi olla tiedonsiirtomäärältään rajoitettua ja yhteysnopeudeltaan hidasta. VPN-palveluita miettiessä ja arvioidessa on suositeltavaa tarkistaa seuraavat seikat: onko palvelun uutisoitu vuotavan tietoja menneisyydessä, mitä salausta ja protokollaa palvelu käyttää, missä maassa palvelimet fyysisesti sijaitsevat ja minkä valtion lakia yritys noudattaa sekä mitkä ovat palvelun tietosuojaehdot erityisesti lokitietojen osalta. Toistaiseksi yksityisyyden suojan kannalta hyvässä maineessa olevia VPN-palveluntarjoajia ovat esimerkiksi IPredator, AirVPN, Mullvad, VPN4All ja Anonine (IPredator 2013, AirVPN 2013, Mullvad 2013, VPN4All 2013, Anonine 2013). Maksullisia palveluita käytettäessä on hyvä pitää mielessä, että myös maksuliikenteestä jää jäljet, joilla käyttäjä voidaan loppujen lopuksi identifioida erityisesti silloin, jos palvelu tallentaa kirjanpitoa maksuliikenteestään. Siksi anonyymimmät maksutavat saattavat joissakin tilanteissa olla aiheellisia. Tällaisia ovat esimerkiksi Bitcoin, Paysafecard ja Liberty Reserve (Bitcoin 2013, Paysafecard 2013, Liberty Reserve 2013).

6.4 Hakukoneet

Internetin käytetyimpiin verkkopalveluihin kuuluvat hakukoneet, jotka indeksoivat verkkosivujen sisällöt ja tarjoavat käyttäjilleen helppokäyttöistä tiedonhakua. Hakukoneista suosituin on Google, joka kasvaessaan on laajentanut palveluvalikoimaansa huomattavasti. Nykyisin Google tarjoaa hakukoneensa lisäksi mm. sähköpostipalvelun, kalenteripalvelun, verkkoselaimen, käyttöjärjestelmän, sosiaalisen median verkon, videopuhelu- ja

pikaviestintäohjelmiston, karttapalveluita, sovelluskaupan sekä asiakirjojen, esitysten ja taulukkolaskentakaavioiden hallintasovelluksia. Käyttäjiä Google on houkutellut tarjoamalla palvelunsa ilmaiseksi. Täysin ilmaiseksi käyttäjät eivät palveluita kuitenkaan saa, vaan samalla he luopuvat yksityisyydestään. Googlen tietosuojaehdoissa kerrotaan seuraavasti (Google 2012):

> Itse antamasi tiedot. Useat palvelumme edellyttävät Google-tilin luomista. Pyydämme sinulta tilin luomisen yhteydessä henkilötietoja, kuten nimesi, sähköpostiosoitteesi, puhelinnumerosi tai luottokorttisi numeron. Jos haluat käyttää kaikkia tarjoamiamme jakamisominaisuuksia, saatamme myös pyytää sinua luomaan julkisesti näkyvillä olevan Google-profiilin, joka voi sisältää nimesi ja valokuvasi.
>
> Palveluidemme käytön kautta saamamme tiedot. Voimme kerätä tietoja käyttämistäsi palveluista ja niiden käyttötavoista, esimerkiksi vieraillessasi mainospalveluitamme käyttävällä sivustolla tai tarkastellessasi ja käyttäessäsi mainoksiamme ja sisältöämme. Näitä tietoja ovat muun muassa:
>
> Laitetiedot: Voimme kerätä laitekohtaisia tietoja (muun muassa koskien laitteiston mallia, käyttöjärjestelmäsi versiota, yksilöllisiä laitetunnisteita sekä käyttämääsi mobiiliverkkoa, mukaan lukien matkapuhelinnumerosi). Google voi yhdistää laitetunnisteesi tai puhelinnumerosi Google-tiliisi.
>
> Lokitiedot: Kun käytät Googlen palveluja tai tarkastelet Googlen tarjoamia tietoja, saatamme automaattisesti kerätä ja tallentaa tiettyjä tietoja palvelinlokeihimme. Nämä tiedot voivat sisältää:
> 1) tiedot siitä, miten käytät palveluitamme (kuten käyttämiäsi hakusanoja).
> 2) puhelulokitietoja, kuten puhelinnumerosi, soittajan numeron, soitonsiirtonumerot, puhelujen kellonajat ja päivämäärät, puhelujen kestot, tekstiviestien reititystiedot ja puhelujen tyypit.
> 3) internetprotokollan osoitteen.
> 4) laitteen käyttötietoja, kuten tietoja mahdollisista kaatumisista, järjestelmän toiminnasta, laitteiston asetuksista, selaintyypistä, selaimen kielestä, kyselysi kellonajasta ja päivämäärästä sekä tähän liittyvästä URL-osoiteviitteestä.
> 5) evästeitä, joiden avulla voimme tunnistaa selaimesi tai Google-tilisi.
>
> Sijaintitiedot: Kun käytät sijaintitietoja hyödyntävää Googlen palvelua, voimme kerätä ja käsitellä todellista sijaintiasi koskevia tietoja, kuten mobiililaitteen lähettämiä GPS-signaaleita. Voimme määrittää sijainnin eri tekniikoiden avulla, kuten hyödyntämällä laitteesi anturidataa, joka voi tarjota tietoja läheisistä langattoman lähiverkon tukiasemista ja radiomastoista.

> Yksilölliset sovellusnumerot: Eräät palvelut sisältävät yksilöllisen sovellusnumeron. Tämä numero ja tietoja asennuksestasi (esimerkiksi käyttöjärjestelmän tyyppi sekä sovelluksen versionumero) voidaan lähettää Googlelle asentaessasi tai poistaessasi kyseisen palvelun tai palvelun ottaessa yhteyttä palvelimiimme esimerkiksi hakiessaan automaattisia päivityksiä.
>
> Paikallinen tallennustila: Voimme paikallisesti kerätä ja tallentaa tietoja (mukaan lukien henkilötietoja) laitteeseesi käyttäen selaimen tallennustilaa (mukaan lukien HTML 5), sovellustietojen välimuistia tai muita vastaavia mekanismeja.
>
> Evästeet ja anonyymit tunnisteet: Käytämme useita erilaisia teknisiä sovelluksia kerätäksemme ja tallentaaksemme tietoa käyttäessäsi Googlen palveluita. Voimme muun muassa lähettää laitteeseesi yhden tai useamman evästeen tai anonyymin tunnisteen. Käytämme evästeitä ja anonyymejä tunnisteita myös käyttäessäsi kumppaneillemme tarjoamiamme palveluita kuten mainospalveluita tai muilla sivustoilla mahdollisesti esiintyviä Google-ominaisuuksia. (Google 2012.)

Tietosuojaehtojensa mukaisesti Google siis ilmoittaa keräävänsä ja hyödyntävänsä käyttäjiensä tietoja suorittaakseen laajamittaista tarkkailua ja yksityiskohtaista profilointia. Koska Googlen tarjoamien palveluiden määrä on mittava ja käyttäjäkunta harvinaisen laaja, voi organisaation palveluista ja tarkkailusta eroaminen tuntua hankalalta. Hakukoneiden suhteen tilanne on kuitenkin positiivinen, koska vaihtoehtoisia ja aidosti yksityisyyden suojaa kunnioittavia palveluita on tarjolla.

Useat hakukoneet tallentavat käyttäjien tekemät hakusanat, hakupäivämäärän kellonaikoineen, IP-osoitteen ja käytettävän selaimen. Tämän lisäksi hakukoneet ujuttavat käyttäjän koneeseen evästetiedostoja ja kuvapistetunnisteita (vrt. luku 3.2). Näillä tiedoilla hakukoneet voivat yksilöidä haun tekijän tarkasti, ja Googlen kaltaiset palvelut voivat myydä tiedot eteenpäin esimerkiksi mainostajille ja tiedonlouhijoille (vrt. luku 2.3) tai luovuttaa ne lainvalvojille sekä tiedustelupalveluille (vrt. luku 2.1).

Käyttäjien yksityisyyden suojaa kunnioittavia hakukoneita ovat mm. DuckDuckGo, Startpage, IxQuick, Gibiru sekä Privatelee. DuckDuckGo (*https://duckduckgo.com*), perustuu omiin hakualgoritmeihinsa ja toimii myös Tor-verkon ulostulosolmuna, jonka ansiosta Tor-verkosta käsin suoritetut haut ovat päästä päähän salattuja ja anonyymejä (vrt. luku 5.1). Hakukonetta voi

käyttää myös välityspalvelimena monille suosituille sivuille, jolloin käytetystä IP-osoitteesta ei jää jälkiä kyseisen sivuston sisäisiin hakuihin. Esimerkiksi YouTube-videopalvelusta voidaan hakea yksityisyyttä käsitteleviä videoita kirjoittamalla DuckDuckGon hakukenttään hakusanaksi *!yt yksityisyys* ja Amazon.co.uk-verkkokaupasta voidaan etsiä yksityisyysaiheisia tuotteita hakusanalla *!auk privacy* (DuckDuckGo 2013a).

IxQuick on metahakukone, joka kerää hakutuloksia samanaikaisesti useista eri hakukoneista säilyttäen kuitenkin käyttäjän yksityisyyden (Ixquick 2013). Startpage on saman organisaation luonnos, mutta se tarjoaa vain Googlen hakutuloksia (Startpage 2013). Gibiru puolestaan tarjoaa omiin hakurobotteihinsa perustuvia hakutuloksia, jotka näyttävät vähemmän tietoja valtavirtaa edustavista verkkosivuista ja suosivat tunnettuja hakukoneita enemmän vaihtoehtoisia sivustoja. Gibirun suodattamaton hakualgoritmi luo lisäksi erillisen sensuroimattoman uutispalstan, joka listaa useita suosittujen hakukoneiden estämiä tai hakutulosten loppupäähän laitettuja sivuja (Gibiru 2013). Privatelee sen sijaan listaa Googlen ja Bingin hakutuloksia keräämättä kuitenkaan tietoja käyttäjästä (Privatelee 2013). Edellä mainittujen hakukoneiden käyttäminen on suositeltavaa yksityisyyden suojan kannalta ja ne tarjoavat perustellun vaihtoehdon suosituimmille hakukoneille.

6.5 Metatieto

Metatieto (engl. *metadata*) on rakenteellista tietoa, joka kuvaa, selittää, paikantaa tai muutoin helpottaa tietolähteen hakemista, käyttämistä tai hallitsemista. Metatieto on siis tietoa tiedosta. Se voidaan sisällyttää digitaaliseen objektiin tai sitä voidaan säilyttää erikseen. Useimmiten metatieto sisällytetään www-sivuihin, kuviin, asiakirjoihin, ääni- ja videotiedostoihin. Sisällyttäminen on hyödyllistä, jottei metatieto häviä ja jotta se on selkeästi liitettävissä sisällytettyyn tietoon. (NISO 2004.)

Metatieto voi olla haitallista, koska se voi paljastaa arkaluontoisia tai muutoin ei-toivottuja asioita tiedon julkaisijasta. Esimerkiksi GPS-paikantimella (*Global*

Positioning System) varustetulla kameralla tai matkapuhelimella otetut valokuvat saattavat paljastaa sijainnin, jossa kuva on otettu, kuvanottamisen ajankohdan sekunnin tarkkuudella sekä laitteen tarkan mallin. Metatiedon poistaminen valokuvista on olennaista varsinkin julkisille verkkosivuille ja sosiaaliseen mediaan julkaistaessa, kun ei haluta paljastaa liikaa henkilökohtaista tietoa. Myös mm. tiedustelupalvelut ja tiedonlouhijat käyttävät metatietoa hyödykseen profiloidessaan kohderyhmiä ja käyttäjiä (vrt. luku 2.3).

Metatiedon poistaminen kuvista onnistuu esimerkiksi Phil Harveyn kehittämällä, ilmaisella ExifTool-ohjelmalla, joka toimii Windows-, GNU/Linux ja Mac OS X-käyttöjärjestelmissä. Sen voi ladata osoitteesta *http://owl.phy.queensu.ca/~phil/exiftool*. Ohjelman asentamisen jälkeen esimerkiksi paikannustietojen poistaminen onnistuu komentoriviltä käsin komennolla *exiftool -a -gps:all kuva.jpg*. Ohjelman kotisivuilta löytyy myös linkkejä graafisiin käyttöliittymiin eri käyttöjärjestelmille, mikä helpottaa ohjelman käyttämistä. (ExifTool 2013.)

6.6 Sähköposti

Sähköpostiviestintä on eräs suosituimmista Internet-verkon palveluista. Viestit lähetetään kuitenkin suojaamattoman SMTP-protokollan (*Simple Mail Transfer Protocol*) ylitse ja sen seurauksena niitä tarkkaillaan useiden valtioiden ja tiedustelupalveluiden toimesta. Kuten luvussa 2.2 todettiin, tämän vuoksi myös EU suosittelee kansalaisilleen sähköpostiviestien salausta. Määritykset Internetin kautta toimivalle sähköpostiliikenteelle voidaan definioida kolmeen kategoriaan taulukon 4 mukaisesti:

Taulukko 4. Sähköpostiviestimisen kolme protokollatyyppiä (Comer 2009, 64).

Tyyppi	Kuvaus
Siirtäminen	Protokolla, jota käytetään sähköpostin siirtämiseen ja välittämiseen
Saatavuus	Protokolla, jonka avulla käyttäjä voi yhdistää sähköpostilaatikkoonsa
Esitys	Protokolla, joka määrittelee sähköpostiviestin muodon

Sähköpostiviestien välittäminen tapahtuu yleensä SMTP-protokollan avulla, mutta joissakin tapauksissa voidaan hyödyntää toisiakin protokollia. Kun esimerkiksi sähköpostin kohde on Internetin ulkopuolella, voidaan käyttää myös muita protokollia. (Schmeh 2003, 359.) Sähköpostiviesteihin käsiksi pääsemiseen tarvitaan omat protokollansa, koska käyttäjän pitää pystyä hallitsemaan sähköposteja sähköpostilaatikossaan. Näitä ovat esimerkiksi POP3 (*Post Office Protocol version 3*) ja IMAP (*Internet Mail Access Protocol*). Viestin esittämiseen käytetään puolestaan sisällön muotostandardeja RFC2822 ja MIME (*Multipurpose Internet Mail Extensions*). (Comer 2009, 67–68.)

Sähköpostilaatikoiden turvaamiseen on kehitelty palvelimen tasolla tuettavia tekniikoita. Näitä POP- ja IMAP-protokollia tukevia laajennuksia ovat mm. Kerberos, GSS-API ja S/Key. Tämän lisäksi kyseiset protokollat voidaan suojata SSL/TLS-protokollalla (vrt. luku 4.4). (Schmeh 2003, 371.) Sähköpostipalvelimen tai -palvelun valinnassa kannattaakin ottaa huomioon, miten varsinainen sähköpostilaatikko suojataan siihen kirjautumisen yhteydessä.

6.6.1 Viestien salaaminen

Koska sähköpostin välittämiseen käytetty SMTP-protokolla on turvaton, on käyttäjän syytä salata ainakin arkaluontoisimmat viestit. Protokolla käsittelee pyyntöjä itsenäisinä tapahtumina, ja siksi salatun tai allekirjoitetun viestin tulee aina sisältää kaikki tarvittavat tiedot sen käsittelemiseen. Tämä merkitsee sitä, että salausavainten vaihtamisen ja salausmenettelyjen toiminnan tulee tapahtua ilman erillisiä viestejä. (Schmeh 2003, 361.)

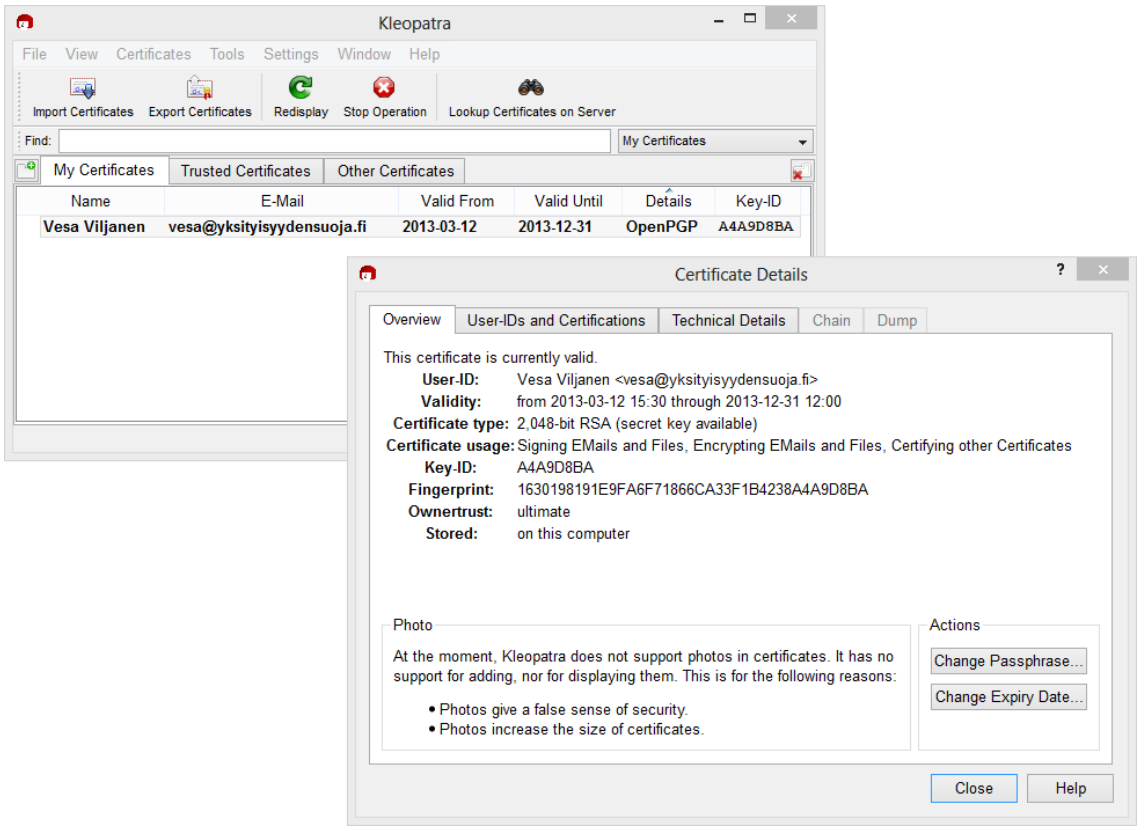
Ensimmäinen salausstandardi sähköpostiviestinnälle, PEM (*Privacy Enhancement for Internet Electronic Mail*) luotiin 1980-luvun puolivälissä. Vanhuudestaan johtuen menetelmän on kuitenkin nykyisin korvannut kolme uudempaa ratkaisua. Nämä ovat Phil Zimmermannin kehittelemästä PGP-salausmenetelmästä (*Pretty Good Privacy*) jatkettu OpenPGP-standardi, RSA Security -yrityksen suunnittelema S/MIME (*Secure MIME*) sekä saksalaisen Teletrust-organisaation hahmottelema Mailtrust. Mailtrust on tarkoitettu Saksan

allekirjoituslain mukaiseen käyttöön, joten se ei ole muissa maissa niin oleellinen ratkaisu. (Schmeh 2003, 361–367.)

OpenPGP yhdistää perinteisen ja julkisen avaimen salauksen. Sähköpostiviestin salaamista varten käyttäjä tarvitsee lisäksi viestin vastaanottajan julkisen avaimen (engl. *public key*). Käyttäjän salatessa selväkielisen tekstin OpenPGP tiivistää salattavan tiedon säästääkseen tilaa sekä vahvistaakseen salauksen turvallisuutta. Tämän jälkeen salauksessa luodaan istuntoavain (engl. *session key*), joka koostuu satunnaisista numeroista. Tällä avaimella salataan selkokielinen teksti, ja varsinainen istuntoavain salataan viestin vastaanottajan julkisella avaimella. (GPGTools 2013.)

Viestin purkaminen puolestaan onnistuu käänteisessä järjestyksessä. Vastaanottaja voi purkaa viestin käyttämällä yksityistä salausavaintaan (engl. *private key*) purkaakseen istuntoavaimen. Istuntoavaimella puolestaan voidaan purkaa varsinainen salattu viesti. Aihepiirin laajuuden vuoksi tässä tutkielmassa ei kuitenkaan käsitellä salausmenetelmien teoriaa tarkemmin, vaan ainoastaan esitellään, kuinka vakiintuneita standardeita voidaan hyödyntää omassa viestinnässä. (GPGTools 2013.)

GnuPG (*Gnu Privacy Guard, GPG*) on ilmainen ja kattava ohjelmistopaketti, joka sisältää OpenPGP-standardin mukaiset salaustyökalut. Sillä voidaan mm. allekirjoittaa, salata ja purkaa sähköpostiviestit ja tiedostot. Ohjelmisto toimii GNU/Linux-käyttöjärjestelmissä, mutta siitä on saatavilla myös Windows- ja Mac OS X-versiot. Ohjelman voi ladata GNU/Linuxille sen kotisivuilta osoitteesta *http://www.gnupg.org*, Windows-version osoitteesta *http://gpg4win.org* ja Mac OS X-version osoitteesta *https://www.gpgtools.org*. Ohjelmapaketin asennuksen jälkeen viestejä voidaan salata OpenPGP:tä hyödyntäen. Nämä vaativat käyttäjältä kuitenkin lisätoimenpiteinä omien sertifikaattien luontia. OpenPGP:tä varten sertifikaatti voidaan luoda käyttämällä GnuPG-pakettiin kuuluvaa Kleopatra-ohjelmaa. Ohjelmassa on ohjattu sertifikaatin luonti, jonka avulla luominen onnistuu helposti. (GnuPG 2013.) Kuva 18 esittää, miltä Kleopatra-ohjelmalla luotu sertifikaatti näyttää tietoineen.



Kuva 18. Kuvakaappaus Kleopatra-sovelluksesta ja OpenPGP-sertifikaatista (Kleopatra 2013).

S/MIME vaatii oman sertifikaatin toimiakseen, mikäli sitä halutaan käyttää sähköpostiviestien salaukseen. Tietoturvayhtiö Comodo tarjoaa sertifikaatin ilmaiseksi, ja sitä voi pyytää osoitteesta *http://www.comodo.com/home/email-security/free-email-certificate.php*. Sertifikaatin pyytämisen jälkeen käyttäjä saa antamaansa sähköpostiosoitteeseen ohjeet, joiden mukaisesti sertifikaatti voidaan tuoda käytettäviin ohjelmiin.

Ilmaisista sähköpostiohjelmista eräs parhaimmista on Mozilla Thunderbird, jonka voi Enigmail-laajennuksen avulla konfiguroida käyttämään sekä OpenPGP:tä että S/MIME:ä. Thunderbird-sähköpostiohjelman voi ladata sen kotisivuilta osoitteesta *https://www.mozilla.org/en/thunderbird* ja Enigmail-laajennuksen voi lisätä joko Thunderbird-ohjelmasta käsin tai ladata osoitteesta *http://www.enigmail.net*. Sekä Thunderbird että Enigmail toimivat GNU/Linux-, Mac OS X- ja Windows-käyttöjärjestelmissä. (Thunderbird 2013, Enigmail 2013.)

6.6.2 Turvalliset sähköpostipalvelut

Sähköpostiviestien salaamisen lisäksi on hyvä tiedostaa, että kaikki sähköpostilaatikossa oleva salaamaton data on sähköpostipalveluntarjoajan katseltavissa. Tämän vuoksi olisi suositeltavaa käyttää yksityisyyden suojaa kunnioittavia sähköpostipalveluita sekä turvata kirjautuminen tarpeeksi vahvoilla salasanoilla (vrt. luku 3.3). Turvallisilla sähköpostipalveluilla tarkoitetaan palveluita, jotka tarjoavat mahdollisuutta sähköpostin tietoturvalliseen säilyttämiseen sekä suojattuun sähköpostilaatikkoon kirjautumiseen. Jos omaan sähköpostipalveluntarjoajaan ei voi luottaa, löytyy Internetistä ilmaisia ja luotettavia palveluita. Tällä hetkellä tietosuojaehdoiltaan ja salausmenetelmiltään suositeltavia sähköpostipalveluita tarjoavat mm. Safe-mail, Xmail ja VFEmail (Safe-mail 2013, Aaex Corp 2013, VFEmail 2013). Kaikki nämä ovat kaupallisia, mutta tarjoavat osittain rajoitettua palveluaan ilmaiseksi. Täysin ilmaista ja anonyymiä sähköpostia tarjoaa mm. Tor Mail, johon voi rekisteröityä ja jota voi käyttää vain Tor-verkossa. Palvelu löytyy Tor-verkon osoitteesta http://jhiwjjlqpyawmpjx.onion, mutta perustietoja palvelusta voi katsella myös Internetistä käsin osoitteesta https://tormail.org (Tor Mail 2013).

PrivacyBox on German Privacy Foundationin tarjoama palvelu, joka mahdollistaa helppokäyttöisen ja anonyymin yhteydenottotavan. Palvelu on ensisijaisesti suunnattu toimittajille, blogin pitäjille ja aktivisteille, mutta se on kaikkien vapaassa käytössä. PrivacyBoxin ideana on antaa kaikille mahdollisuus lähettää viestejä ilman, että kukaan pystyy jäljittämään alkuperäisen viestin lähettäjää. Palvelu toimii siten, että vastaanottaja luo tilin pseudonyymillään PrivacyBoxiin, jolloin hän saa neljä erilaista yhteydenottolinkkiä. Ensimmäinen linkki on normaali URL-osoite, toinen linkki on puhelimissa toimiva .mobi-päätteinen URL-osoite, kolmas linkki on TOR-verkon alla toimiva .onion-osoite ja neljäs linkki on I2P-verkossa toimiva .i2p-päätteinen URL-osoite. Osoitteiden avulla lähettäjä voi jakaa useita yhteydenottomahdollisuuksia, joista viestin lähettäjä voi valita haluamansa. Näiden lisäksi palvelulla voidaan lähettää viestejä pelkällä pseudonyymillä PrivacyBoxin sivuilla joko Internetissä tai anonyymeissä verkoissa. Viesteihin on mahdollista liittää maksimissaan 600 kilotavun liitetiedostoja. (PrivacyBox 2012.)

Vastaanottaja voi halutessaan ottaa käyttöönsä lisätoiminnon, joka lähettää saapuneet viestit uudelleen ilman tunnistetietoja vastaanottajan määrittelemään sähköpostiosoitteeseen. Automaattinen uudelleenlähetys on mahdollista salata OpenPGP-avaimella tai käyttämällä S/MIME-sertifikaattia (vrt. luku 6.6.1). PrivacyBox väittää, ettei palvelu kirjaa viestien lähettäjästä mitään tietoa, eikä voi siksi vuotaa niitä kenellekään. Palvelun huonona puolena on, että viestiminen toimii vain yhteen suuntaan, eli viesteihin ei voi vastata. Käyttäjätilin luvataan olevan poistettavissa kokonaan, jolloin kaikki tieto tuhotaan saman tien ja varmuuskopioidut tiedot hävitetään tunnin sisällä tilin sulkemisesta. (PrivacyBox 2012.)

6.7 Pikaviestintä

Pikaviestimillä eli pikaviestintäohjelmilla tarkoitetaan tietokoneohjelmia, jotka sallivat reaaliaikaisen viestinnän eri osapuolten välillä. Tunnetuimpia pikaviestintäohjelmia ovat mm. Skype sekä siihen yhdistynyt Windows/MSN Live Messenger, Pidgin, Trillian, Facebook Messenger, iChat ja Google Talk. Suurin osa pikaviestintäohjelmista tukee useampia pikaviestintäyhteyksiä ja -verkkoja, mutta osa on tarkoitettu vain tiettyjen verkkojen kautta viestimiseen. Pikaviestintä on suosittua, mutta useat palvelut ja viestintäsovellukset eivät suojaa kokonaisvaltaisesti käyttäjiensä viestintää. Viestiliikenne kulkeekin pahimmassa tapauksessa selkokielisenä tekstinä, jolloin se on helposti ulkopuolisten poimittavissa.

Skype käyttää 256-bittistä AES-salausmenetelmää (vrt. luku 3.4) salatakseen kaiken Skype-ohjelmien välillä kulkevan ääni-, video- ja pikaviestiliikenteen. Skypen palvelimet sertifioivat käyttäjien julkiset avaimet käyttämällä 1536- tai 2048-bittisiä RSA-sertifikaatteja. (Skype 2013a.) Skypen tietosuojaehtojen 12. kohdassa (Skype 2013b) mainitaan seuraavasti pikaviestikeskustelujen tietojen säilyttämisestä:

> Miten kauan Skype säilyttää käyttäjän henkilötietoja?
>
> Se, kuinka kauan Skype säilyttää käyttäjän henkilötietoja, määräytyy seuraavien seikkojen mukaisesti: (1) onko säilyttäminen tarpeen, jotta täytetään tietosuojakäytännön kohdassa 2 mainitut tavoitteet, tai jotta (2) noudatetaan sovellettavaa lainsäädäntöä, viranomaisten pyyntöjä tai toimivaltaisten oikeusistuinten antamia määräyksiä.
>
> Pikaviestien, ääniviestien ja videoviestien säilyttäminen (vain Skypen internetviestintäohjelmisto)
>
> Skype voi säilyttää pikaviestikeskustelujen, ääniviestien ja videoviestien (yhteisesti "viestit") sisällön, (a) jotta viestit voidaan toimittaa ja synkronoida, ja (b) jotta käyttäjä voi halutessaan hakea viestit ja tarkastella niiden historiatietoja. Skype säilyttää viestejä yleensä enintään 30–90 päivän ajan viestin tyypistä riippuen, ellei lainsäädännössä sallita tai edellytetä muuta. Näin viestit voidaan toimittaa, kun käyttäjä on offline-tilassa, ja ne voidaan synkronoida käyttäjän laitteiden kesken. Jos käyttäjä on linkittänyt Skype- ja Microsoft-tilinsä, käyttäjä voi mahdollisesti halutessaan säilyttää koko pikaviestihistoriansa pidemmän aikaa. Tällöin pikaviestit säilytetään Outlook.comin viestikansiossa, kunnes viestit poistetaan manuaalisesti. Käyttäjä voi säilyttää myös videoviestit pidemmän aikaa, jos lähettäjä on Premium-jäsen.
>
> Skype suojaa käyttäjän tietoja asianmukaisilla suojaus- ja teknisillä toimenpiteillä. Käyttämällä tätä tuotetta käyttäjä antaa luvan pikaviestiensä, ääniviestiensä ja videoviestiensä tallentamiseen yllä kuvatuilla tavoilla. (Skype 2013b.)

Skypen tietosuojaehtojen (Skype 2013b) kolmas kohta puolestaan kertoo Skypen keräämien tietojen jakamisesta näin:

> Skype voi paljastaa henkilötietoja noudattaakseen lain vaatimuksia, harjoittaakseen lainmukaisia oikeuksiaan tai puolustautuakseen oikeuskanteilta, suojellakseen Skypen etuja, torjuakseen petoksia ja toimeenpannakseen omia käytäntöjään tai suojellakseen kenen tahansa oikeuksia, omaisuutta tai turvallisuutta. (Skype 2013b.)

Microsoft siis säilyttää Skypen viestintätiedot, suorittaa viestien salauksen itse ja luovuttaa tietoja ulkopuolisille edellä mainituilla ehdoilla. Tietosuojaehdoista voidaan päätellä, että Skypen pikaviestintäyhteyksiä voidaan tarkkailla, ja Skype voi luovuttaa tietojaan ulkopuolisille. Esimerkiksi viranomaiset voivat pyytää käyttäjien tietoja Microsoftilta. Microsoftin julkaiseman raportin mukaan vuoden 2012 aikana Skypen tietoja luovutettiin Suomen viranomaisille seitsemän kertaa ja ne koskivat yhdeksää eri käyttäjätiliä. Suomen viranomaisille jaettiin myös 56

kertaa muita Microsoftin ohjelmia ja palveluita koskevia tietoja, jotka koskivat yhteensä 328 käyttäjää tai käyttäjätiliä. (Microsoft 2013.)

Vaikka pikaviestintä on usein osittain salattua, vain harva palvelu tai ohjelma tukee kunnollista käyttäjältä toiselle käyttäjälle saakka kulkevaa salausta, joka tarjoaisi luotettavan ja turvallisen tavan viestimiselle. Pikaviestintää suojelemaan on siksi kehitelty omia protokollia ja menetelmiä, joista merkittävimmät ovat SILC (*Secure Internet Live Conferencing*) sekä OTR (*Off-the-Record Messaging*) (SILC 2012, Off-the-Record Messaging 2013). OTR on kuitenkin tavallisten käyttäjien kannalta keskeisempi kuin SILC, koska se on helppo asentaa ja liittää sitä tukeviin pikaviestintäohjelmiin.

OTR tarjoaa tehokkaan yksityisyyden suojan pikaviestintäohjelmien välillä salaamalla lähetettävät viestit keskustelun osapuolten välillä. Pikaviestintäohjelman kautta käyttäjä voi ilmoittaa kahdella tavalla, että hän on halukas käyttämään OTR-protokollaa keskustelussa. Keskustelukumppanille voidaan joko lähettää OTR-tiedusteluviesti tai viestiin voidaan sisällyttää erityinen tagi (engl. *tag*), joka koostuu tyhjistä merkeistä. Kummallakin menetelmällä vastaanottaja saa tiedon siitä, millä OTR-protokollan versiolla keskustelu halutaan aloittaa. (Off-the-Record Messaging 2013.)

Pikaviestimistä Jitsi ja Adium tukevat suoraan OTR-salausta, mutta salaus on saatavissa erillisen lisäosan avulla myös joihinkin muihin pikaviestintäohjelmiin (Jitsi 2013, Adium 2013). Esimerkiksi Pidgin osaa hyödyntää OTR-lisäosaa. (Pidgin 2013).

Salattu pikaviestiminen onnistuu myös pelkän selaimen ja Cryptocat-selainlaajennuksen avulla. Tuettuja selaimia ovat toistaiseksi Chrome, Firefox ja Safari. Cryptocatin voi ladata osoitteesta *https://crypto.cat* ja laajennuksen asentamisen jälkeen sen voi käynnistää valitsemalla selaimeen ilmestyneen cryptocat-pikakuvakkeen. Käyttäjältä pyydetään tämän jälkeen keskustelun nimi ja pseudonyymi. Jos keskustelun nimeä ei ole vielä luotu, voidaan se luoda kirjoittamalla kenttään nimi ja kertomalla valittu nimi viestintäkumppanilleen. Kun

keskusteluyhteys muodostetaan, Cryptocat luo keskustelulle salausavaimet ja kaikki viestit salataan OTR:llä. (Cryptocat 2013.)

7 Yhteenveto

Tietoverkkojen käyttäjiä tarkkaillaan jatkuvasti jonkin tahon toimesta. Hakukoneiden hakutiedot, verkkosivujen kohdennetut mainokset, käyttäjän toimia jäljittävät evästeet, sosiaalisen median informaatio, haittaohjelmat, Internet-palveluntarjoajien säilyttämät teletunnistetiedot ja monet muut asiat tarjoavat laajan ja arvokkaan tarkkailuverkoston. Käyttäjien yksityisyyttä ei arvosteta, vaan kaikki tieto tuntuu olevan kaupan. Yksityisyyden suojasta huolehtiminen vaatii nykyisin uusien tapojen omaksumista ja taitoa henkilökohtaisen tiedon varjelemiseen. Tämä lisää huomattavasti vaivannäköä ja saattaa toisinaan tuntua turhauttavalta.

Tutkielmassa tarkasteltiin tietoverkkojen yksityisyyden suojan merkitystä kotikäyttäjälle ja esiteltiin erilaisia keinoja yksityisyyden edistämiseen. Tavoitteena oli löytää erilaisia ratkaisuja yksityisyyden suojan parantamiseksi ja esitellä niiden toteuttamista käytännössä. Työssä käsiteltiin aluksi lainsäädännön vaikutusta yksityishenkilön yksityisyyden suojaan ja sen merkitystä kotikäyttäjälle sekä selvitettiin hieman tahoja, jotka hyödyntävät tarjolla olevaa informaatiota. Tämän jälkeen siirryttiin konkreettisempiin keinoihin, joilla yksityisyyttä voidaan parantaa tietoverkoissa ja esiteltiin erilaisia menetelmiä suojaamisen mahdollistamiseksi.

Tietoturvasta huolehtiminen on perusta tehokkaalle suojautumiselle. Ajantasaisten virustorjunta- sekä palomuuriohjelmistojen käyttäminen ehkäisee useita verkkorikollisten aiheuttamia vaaratilanteita ja on siksi oleellinen osa hyvää tietoturvaa. Verkkoselainten asetuksia muuttamalla ja niihin asennettavien laajennusten avulla voidaan ehkäistä monia www-sivuista käsin tapahtuvia tarkkailu- ja kaappausyrityksiä. Tietotekniikan kehittyessä lyhyiden ja yksinkertaisten salasanojen murtaminen on nopeutunut, minkä vuoksi

tehokkaiden salasanojen käyttämiseen on syytä kiinnittää huomiota. Arkaluontoiset tiedot on tarpeellista salata varkauksien ja verkkohyökkäysten takia, jotta tiedot eivät joutuisi vääriin käsiin. Tämän vuoksi myös tarpeettomien, mutta henkilökohtaisten tai muutoin salaisten, tietojen turvallinen hävittäminen on edellytys hyvälle tietoturvalle.

Asioiden syventämisen ja selkeyttämisen vuoksi työssä käytiin läpi myös oleellisimmat verkkoprotokollat, jotka vaikuttavat käyttäjien yksityisyyden suojaan. Esimerkiksi verkkosivuja selaillessa on järkevämpää käyttää salattua HTTPS-yhteyttä perinteisen HTTP:n tilalla aina, kun palvelin sitä tukee. Julkisia nimipalvelimia voidaan puolestaan hyödyntää, jotta saadaan peitettyä haettujen verkko-osoitteiden selvityspyyntöjä omalta Internet-palveluntarjoajalta. Lopullinen peittäminen vaatii lisäksi oman yhteyden kierrättämisen esimerkiksi VPN-palvelun kautta.

Anonyymit verkot tarjoavat mahdollisuuden oman verkkoidentiteetin piilottamiseen sekä pääsyn vaihtoehtoisiin informaatiolähteisiin. Niiden käyttäminen on olennaista silloin, kun halutaan selailla anonyymisti www-sivuja tai verkkojen omia, piilotettuja sivuja. Ne ovat hyödyllisiä myös anonyymiin kommunikointiin ja tiedon julkaisemiseen. Verkkojen käyttäminen voidaan kokea toisinaan eettisesti arveluttavana, mutta yksityisyyden suojan näkökulmasta ne tarjoavat turvallisen, vaikkakin usein hitaamman vaihtoehdon muille ratkaisuille.

Viimeisenä kokonaisuutena tutkielmassa paneuduttiin viestinnän suojaamiseen erilaisia menetelmiä, ohjelmia ja palveluita hyväksi käyttäen. Yksityisyyden suojaa edistämään on luotu erilaisia käyttöjärjestelmiä, jotka ovat valmiiksi konfiguroituja tietoturvallisuuden ja anonymiteetin varmistamiseksi. Näiden käyttäminen mahdollistaa suojatun viestinnän varsinkin epäluotettavissa olosuhteissa. Tietokoneen IP-osoitteet mahdollistavat käyttäjän jäljittämisen ja yksilöimisen, minkä vuoksi sen estämiseen tarkoitettujen palveluiden käyttöä kannattaa harkita. Näitä ovat mm. välityspalvelimet, VPN-ratkaisut ja Tor-verkko. Useat suositut hakukoneet yksilöivät käyttäjät ja tallentavat heidän suorittamat haut tietokantoihinsa. Nämä tiedot myydään eteenpäin mm. mainostajille.

Ratkaisuna tähän ongelmaan esitetään yksityisyyttä arvostavia hakukoneita, jotka eivät kerää käyttäjien tietoja.

Tutkielmassa käsiteltiin myös metatiedon merkitystä yksityisyyden suojalle. Tiedostoihin tallentuu niiden luomisen yhteydessä usein metatietoja, jotka saattavat paljastaa liikaa tietoja käyttäjästä tai arkaluontoisista asioista. Näitä ovat esimerkiksi valokuvat, joihin saattavat tallentua GPS-sijaintitiedot. Tämän vuoksi tutkielmassa esiteltiin yksi tehokas ohjelma metatiedon poistamiseen. Lopuksi selvitettiin sähköpostin ja pikaviestinnän salaamista ja tarkasteltiin vaihtoehtoisia tapoja turvatun viestinnän luomiseksi. EU suosittelee kansalaisilleen sähköpostiviestinnän salaamista, koska viestit liikkuvat turvattomasti ja niitä tarkkaillaan useiden valtioiden toimesta. Tämän vuoksi sähköpostin salaaminen on tärkeä toimenpide, joka olisi hyvä ottaa yleiseksi tavaksi.

Tietotekniikan, tietoverkkojen ja ohjelmistojen kehittyessä edellä esitetyn informaation voidaan ainakin osin olettaa vanhenevan muutamien vuosien kuluessa. Tämän vuoksi tutkimusta ja tiedonkeruuta on tarkoitus jatkaa, ja uutta tietoa aiheesta julkaistaan jatkossa osoitteessa www.yksityisyydensuoja.fi. Tietoverkot ovat luotu vapaata informaation hakemista ja levittämistä varten, ja kaikilla tulisi olla mahdollisuus etsiä, löytää ja jakaa tietoa ilman pelkoa yksityisyyden suojansa menettämisestä.

Lähteet

Aaex Corp. 2013. XMail. https://xmail.net. 14.4.2013.

Adium. 2013. About Adium. http://adium.im/about. 14.4.2013.

Ahmia. 2013. Tor Hidden Service (.onion) search. https://ahmia.fi/address. 11.4.2013.

AirVPN. 2013. AirVPN – The air to breathe the real Internet. https://airvpn.org. 15.4.2013.

Anonine. 2013. Become Anonymous with Anonine VPN! https://www.anonine.com. 15.4.2013.

Aplin Software. 2012. How Neo's SafeKeys v3 Works. http://www.aplin.com.au/neos-safekeys-v3/how-neos-safekeys-v3-works. 9.11.2012.

Aycock, J. 2006. Computer viruses and malware. New York: Springer Science+Business Media, LLC.

Bitcoin. 2013. An open source P2P digital currency. http://bitcoin.org. 15.4.2013.

Bitvise. 2013. https://www.bitvise.com. 10.4.2013.

Burnett, M. & Kleiman, D. 2006. Perfect passwords – Selection, protection, authentication. Rockland: Syngress Publishing, Inc.

Chaos Computer Club. 2011. Chaos Computer Club analyzes government malware. http://www.ccc.de/en/updates/2011/staatstrojaner. 4.11.2012.

Comer, D. E. 2009. Computer Networks and Internets. New Jersey: Pearson Education, Inc.

Comodo. 2013. Comodo Secure DNS - Enjoy a safer, smarter and faster Internet. http://www.comodo.com/secure-dns. 7.3.2013.

Craig, T. & Ludloff, M. E. 2011. Privacy and big data. Sebastopol: O'Reilly Media Inc.

Cryptocat. 2013. Cryptocat lets you chat with privacy. https://crypto.cat. 11.4.2013.

Darik's Boot And Nuke. 2013. About DBAN. http://dban.org. 10.4.2013.

Direktiivi tunnistamistietojen tallentamisesta 24/2006/EY.

DiskCryptor. 2013. DiskCryptor – Open source partition encryption solution. http://diskcryptor.net/wiki/Main_Page/en. 14.4.2013.

Diskscrub. 2013. Diskscrub – Disk overwrite utility. https://code.google.com/p/diskscrub. 11.4.2013.

Dormann, W. & Rafail J. 2008. Securing Your Web Browser. CERT. https://www.cert.org/tech_tips/securing_browser. 18.2.2013.

Dr.Web. 2012. The first Trojan in history to steal Linux and Mac OS X passwords. http://news.drweb.com/show/?i=2679. 10.11.2012.

DuckDuckGo. 2013a. !Bang. https://duckduckgo.com/bang.html. 8.3.2013.

DuckDuckGo. 2013b. How-to stop getting tracked in your browser. http://fixtracking.com 13.4.2013.

Electronic Frontier Foundation. 2013a. HTTPS Everywhere. https://www.eff.org/https-everywhere. 18.2.2013.

Electronic Frontier Foundation. 2013b. Surveillance Self-Defense – Tor. https://ssd.eff.org/tech/tor. 8.3.2013.

Enigmail. 2013. A simple interface for OpenPGP email security. http://www.enigmail.net/home/index.php. 12.4.2013.

Eraser. 2013. http://eraser.heidi.ie. 10.4.2013.
EYVL. 2002. Euroopan parlamentin päätöslauselma yksityistä ja talouselämän viestintää sieppaavan maailmanlaajuisen järjestelmän (Echelon-sieppausjärjestelmän) olemassaolosta (2001/2098(INI)). Euroopan yhteisöjen virallinen lehti, 21.3.2002, 45. vsk, nro C 72 E. Euroopan unionin julkaisutoimisto. S. 221–229. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2002:072E:0221:0229:FI:PDF. 6.11.2012.
ExifTool. 2013. ExifTool by Phil Harvey – Read, Write and Edit Meta Information! http://owl.phy.queensu.ca/~phil/exiftool. 11.4.2013.
Feilner, M. 2006. OpenVPN Building and Integrating Virtual Private Networks. Birmingham: Packt Publishing Ltd.
Facebook. 2012. Tietojenkäyttökäytäntö. 8.6.2012. https://fi-fi.facebook.com/about/privacy/your-info. 26.3.2013.
Farivar C. 2011. German company behind government spyware admits sale to Bavaria. Deutsche Welle. 11.10.2011. http://www.dw.de/german-company-behind-government-spyware-admits-sale-to-bavaria/a-15453150-1. 7.11.2012.
Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FISAA), Pub. L. No. 110-261, 2008. http://www.gpo.gov/fdsys/pkg/PLAW-110publ261/pdf/PLAW-110publ261.pdf. 14.1.2013.
Freenet. 2013. What is Freenet? https://freenetproject.org/whatis.html. 10.3.2013.
Gibiru. 2013. Gibiru – Uncensored Anonymous Search. https://anonymous-gibiru.com. 14.4.2013.
Glype. 2013. Glype – proxy script. https://www.glype.com 13.4.2013.
GnuPG. 2013. The GNU Privacy Guard. http://www.gnupg.org. 11.4.2013.
Google. 2013. Public DNS. https://developers.google.com/speed/public-dns. 7.3.2013.
Google. 2012. Tietosuojakäytäntö. 27.7.2012. https://www.google.com/intl/fi/policies/privacy. 8.3.2013.
GPGTools. 2013. Introduction to Cryptography. http://support.gpgtools.org/kb/how-to/introduction-to-cryptography. 15.4.2013.
Henkilötietodirektiivi 46/1995/EY.
Henkilötietolaki 523/1999.
Hughes G. & Coughlin T. 2008. Tutorial on Disk Drive Data Sanitization. http://cmrr.ucsd.edu/people/Hughes/DataSanitizationTutorial.pdf. 27.2.2013.
Hyppönen M. 2011. Three types of online attack. http://www.ted.com/talks/mikko_hypponen_three_types_of_online_attack.html. 4.11.2012.
Hyppönen M. 2012. Why Antivirus Companies Like Mine Failed to Catch Flame and Stuxnet. 1.6.2012. http://www.wired.com/threatlevel/2012/06/internet-security-fail. 3.3.2013.
I2P. 2012. Introducing I2P. http://www.i2p2.de/techintro.html. 4.11.2012.
InformAction. 2013. NoScript. http://noscript.net. 11.4.2013.
IPredator. 2013. VPN. https://www.ipredator.se. 15.4.2013.
Ixquick. 2013. Ixquick – the world's most private search engine. https://ixquick.com. 14.4.2013.

JAP Anonymity & Privacy. JonDonym, AN.ON and Tor. http://anon.inf.tu-dresden.de/help/jap_help/en/help/jondonym.html. 8.3.2013.
Jitsi. 2013. Jitsi – Open Source Video Calls and Chat. https://jitsi.org. 14.4.2013.
JonDonym. 2013a. FAQ JonDo. https://anonymous-proxy-servers.net/en/faq-jondo.html. 8.3.2013.
JonDonym. 2013b. Jondonym Private and Secure Web Surfing. https://anonymous-proxy-servers.net. 8.3.2013.
InsidePro. 2012. Extreme GPU bruteforcer. http://www.insidepro.com/eng/egb.shtml. 9.11.2012.
Jowitt T. 2011. HideMyAss Anonymous VPN Shops Lulzsec Suspects. 26.9.2011. http://www.techweekeurope.co.uk/news/hidemyass-anonymity-service-exposes-alleged-lulzsec-hackers-40663. 6.3.2013.
Kaspersky. 2012. Kaspersky Security Bulletin 2012. The overall statistics for 2012. https://www.securelist.com/en/analysis/204792255/Kaspersky_Security_Bulletin_2012_The_overall_statistics_for_2012. 7.3.2013.
KeePass. 2013. KeePass – Password Safe. http://keepass.info. 14.4.2013.
Kerner. S. M. 2013. Chrome, Firefox and IE Fall at Pwn2Own 2013. http://www.esecurityplanet.com/browser-security/chrome-firefox-and-ie-fall-at-pwn2own-2013.html. 10.3.2013.
Kleopatra. 2013. Kleopatra – Certificate Manager and Unified Crypto GUI. http://www.kde.org/applications/utilities/kleopatra. 10.4.2013.
Kotimaisten kielten keskus. 2007. Kotimaisten kielten keskuksen nykysuomen sanalista. http://kaino.kotus.fi/sanat/nykysuomi. 15.03.2013.
Lag om signalspaning i försvarsunderrättelseverksamhet 2008:717. https://lagen.nu/2008:717. 4.11.2012.
Laki viranomaisten toiminnan julkisuudesta 621/1999.
Laki yksityisyyden suojasta työelämässä 759/2004.
LastPass. 2013. LastPass – The Last Password You'll Have to Remember! https://lastpass.com. 14.4.2013.
Lee M. 2012. Privacy in Ubuntu 12.10: Full Disk Encryption. https://www.eff.org/deeplinks/2012/11/privacy-ubuntu-1210-full-disk-encryption. 7.11.2012.
Liberté Linux. 2012. Summary. http://dee.su/liberte. 28.12.2012.
Liberty Reserve. 2013. http://www.libertyreserve.com. 15.4.2013.
McCullagh D. 2012. FBI: We need wiretap-ready Web sites – now. CNET. http://news.cnet.com/8301-1009_3-57428067-83/fbi-we-need-wiretap-ready-web-sites-now. 4.11.2012.
Menn J. 2012. Social networks scan for sexual predators, with uneven results. Reuters. http://www.reuters.com/article/2012/07/12/us-usa-internet-predators-idUSBRE86B05G20120712. 4.11.2012.
Microsoft. 2013. Law Enforcement Requests Report. http://download.microsoft.com/download/F/3/8/F38AF681-EB3A-4645-A9C4-D4F31B8BA8F2/MSFT_Reporting_Data.pdf. 24.3.2013.
Mozilla. 2013. Thunderbird. https://www.mozilla.org/fi/thunderbird. 12.4.2013.
Mullvad. 2013. Communicate anonymously and without getting spied on. https://mullvad.net. 15.4.2013.
NISO. 2004. Understanding Metadata. National Information Standards Organization.

http://www.niso.org/publications/press/UnderstandingMetadata.pdf. 8.3.2013.
Off-the-Record Messaging. 2013. Off-the-Record Messaging Protocol version 3. http://www.cypherpunks.ca/otr/Protocol-v3-4.0.0.html. 9.3.2013.
OpenSSH. 2013. OpenSSH – Keeping your communiqués secret. http://www.openssh.com. 10.4.2013.
Password Safe. 2013. Password Safe – Simple & Secure Password Management. http://passwordsafe.sourceforge.net. 14.4.2013.
Paysafecard. 2013. Paysafecard – pay cash. pay safe. https://www.paysafecard.com. 15.4.2013.
Pidgin. 2013. About Pidgin. http://pidgin.im/about. 14.4.2013.
Pierce D. & Ackerman L. 2005. Data Aggregators: A Study of Data Quality and Responsiveness. http://web.archive.org/web/20070319220412/http://www.privacyactivism.org/docs/DataAggregatorsStudy.html. 4.11.2012.
PrivacyBox. 2012. Description of the PrivacyBox. https://privacybox.de. 4.11.2012.
Privatelee. 2013. https://privatelee.com. 14.4.2013.
QFX Software Corporation. 2013. KeyScrambler. A Breakthrough in Securing User Info Against Keylogging. http://www.qfxsoftware.com/ks-windows/how-it-works.htm. 14.4.2013.
Rogin J. 2012. Eric Schmidt: The Great Firewall of China will fall. Foreign Policy. 9.7.2012. http://thecable.foreignpolicy.com/posts/2012/07/09/eric_schmidt_the_great_firewall_of_china_will_fall. 6.11.2012.
Rott J. 2012. Intel Advanced Encryption Standard Instructions (AES-NI). http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni. 26.2.2013.
RSA. 2012. Information Security Glossary: two factor authentication. https://www.rsa.com/glossary/default.asp?id=1056. 9.11.2012.
RT. 2013. Cloud surfing: US surveilance act ‘grave threat’ to EU sovereignty. https://rt.com/news/fisa-spy-eu-cloud-619. 10.1.2013.
Safe-mail. 2013. Welcome to Safe-mail. https://www.safe-mail.net. 14.4.2013.
Sanastokeskus TSK. 2004. Tiivis Tietoturvasanasto. Helsinki: Sanastokeskus TSK ry. http://www.tsk.fi/fi/info/TiivisTietoturvasanasto.pdf. 4.11.2012.
Sandboxie. 2013. Introducing Sandboxie. http://www.sandboxie.com. 11.4.2013.
Schmeh, K. 2003. Cryptography and public key infrastructure on the Internet. Chichester: John Wiley & Sons Ltd.
SILC. 2012. SILC – Secure Internet Live Conferencing. http://silcnet.org. 14.4.2013.
Singer N. 2012. You for Sale: Mapping, and Sharing, the Consumer Genome. The New York Times. 16.6.2012. http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html. 4.11.2012.
Skype. 2013a. Privacy and security: Does Skype use encryption. https://support.skype.com/en/faq/FA31/does-skype-use-encryption. 28.2.2013.
Skype. 2013b. Skypen tietosuojakäytäntö. http://www.skype.com/fi/legal/privacy. 28.2.2013.

SpyShelter. 2012. Stop-Logger – Protect your privacy and feel secure. http://www.spyshelter.com/description. 14.4.2013.
SSH Communications Security. 2013. SSH – Securing the path to your information assets. http://www.ssh.com. 10.4.2013.
SSL Proxy. 2013. https://www.proxyssl.org. 13.4.2013.
Stallings, W. 2011. Cryptography and network security – Principles and practice. 5th edition. New York: Pearson Education, Inc.
Startpage. 2013. Startpage – the world's most private search engine. https://startpage.com. 14.4.2013.
Stecklow S. 2012. Special Report: Chinese firm helps Iran spy on citizens. Reuters 22.3.2012 http://www.reuters.com/article/2012/03/22/us-iran-telecoms-idUSBRE82L0B820120322. 6.11.2012.
Stewart, J. M. 2011. Network Security, firewalls, and VPNs. Lontoo: Jones & Bartlett Learning, LLC.
Stuttard, D. & Pinto, M. 2011. The web application hacker's handbook. Indianapolis: John Wiley & Sons, Inc.
Suomen perustuslaki 731/1999.
Symantec. 2012. Vulnerability Trends. https://www.symantec.com/threatreport/topic.jsp?id=vulnerability_trends&aid=web_browser_vulnerabilities. 18.2.2013
Sähköisen viestinnän tietosuojadirektiivi 58/2002/EY.
Sähköisen viestinnän tietosuojalaki 516/2004.
Sähköisen viestinnän tietosuojalain säädös 343/2008.
Tails. 2013. Tails – The amnesic incognito live system. https://tails.boum.org. 10.4.2013.
The Tor Project. 2013. Tor: Overview. https://www.torproject.org/about/overview.html.en. 18.2.2013.
Tor Mail. 2013. Tor Mail is a free anonymous email service provider. http://tormail.org. 11.4.2013.
Tor2web. 2013. Tor2web: visit anonymous websites. http://tor2web.org. 15.3.2013.
TrueCrypt Foundation. 2013. TrueCrypt – Free open-source on-the-fly encryption. http://www.truecrypt.org. 10.4.2013.
Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, 2001. http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf. 4.11.2012.
Valtiovarainministeriö. 2008. Valtionhallinnon tietoturvasanasto. Helsinki: Edita Prima Oy. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20081211Valtio/Vahti_8_NETTI%2b_KANNET.pdf. 4.11.2012.
Viestintävirasto. 2007a. Palomuuri. http://web.archive.org/web/20130117161236/http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/palomuuri.html. 9.11.2012.
Viestintävirasto. 2007b. Virustorjunta. http://web.archive.org/web/20130117161341/http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/virustorjunta.html. 9.11.2012.
Viestintävirasto. 2009. Salausmenetelmät. http://web.archive.org/web/20130117161208/http://www.ficora.fi/inde

x/palvelut/palvelutaiheittain/tietoturva/salausmenetelmat.html. 4.11.2012.
Viestintävirasto. 2013. Usein kysytyt kysymykset. https://domain.fi/info/index/tietoa/useinkysytytkysymykset.html. 7.3.2013.
VFEmail. 2013. http://vfemail.net. 14.4.2013.
VirtualBox. 2013. https://www.virtualbox.org. 10.4.2013.
VPN4All. 2013. Encrypt your internet and change your IP address. https://www.vpn4all.com. 15.4.2013.
Whonix. 2013. Whonix – Anonymous operating system. http://sourceforge.net/p/whonix/wiki/Home. 10.4.2013.
Zemana 2013. Zemana AntiLogger. http://www.zemana.com/product/antilogger/overview. 14.4.2013.
Zuckerberg M. 2012. One billion people on Facebook. http://newsroom.fb.com/News/457/One-Billion-People-on-Facebook. 15.3.2013. Ladattava tiedote. http://newsroom.fb.com/download-media/4227. 15.3.2013.