Jani Tenhivaara

Matkailijan tietoturvapaketti

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tieto- ja viestintätekniikan tutkinto-ohjelma

Insinöörityö

20.4.2018

Metropolia

Tekijä Otsikko Sivumäärä Aika	Jani Tenhivaara Matkailijan tietoturvapaketti 38 sivua 20.4.2018
Tutkinto	Insinööri (AMK)
Tutkinto-ohjelma	Tieto- ja viestintätekniikka
Ohjaajat	Osaamisaluepäällikkö Janne Salonen

Insinöörityön tarkoituksena on tutkia matkailijalle kohdistuvia tietoturvauhkia ja sitä, miten näihin uhkiin voi varautua. Nykyään tietotekniikan käyttäminen ja siihen tukeutuminen on hyvin laajaa, mutta tietotekniikkaan suuntautunut rikollisuus on myös kasvamassa. Tietoturvalla perinteisesti tarkoitetaan tiedon luotettavuutta, saatavuutta ja eheyttä. Tietoturvaan nykyään lisätään myös tiedon todentaminen ja kiistämättömyys.

Insinöörityö on jakautunut neljään osaan. Ensimmäisessä osassa käyn läpi yleisempiä tietoturvauhkia matkailijalle. Toisessa osassa käyn läpi miten tietoturvauhkia voi välttää. Kolmannessa osassa otan esille käytännön ohjelmia ja menetelmiä tietoturvaan liittyen ja tuon esille näiden ominaisuuksia. Viimeisessä osassa luon vaiheittaisen ohjeen jo käytössä olevien tietokoneen ja puhelimen tietoturvan parantamiseen, miten luoda uusi turvallinen Ubuntu-käyttöjärjestelmä ja miten ottaa käyttöön tietoturvallisuuteen perustuvan käyttöjärjestelmä, Tails, USB-muistilaitteelle.

Matkailijan on syytä turvata oma tieto jo ennen matkaa, mutta myös matkalla ja matkan jälkeen tulee ylläpitää omaa tietoturvaansa. Hyökkääjinä matkailijan tietoturvalle voi olla yksityisten henkilöiden lisäksi hallituksien virastot. Snowdenin paljastusten mukaan hallitusten virastot voivat olla tietoturvauhka epäsuoraankin, koska he heikentävät salausprotokollia. Laajalti ja oikein tehdyt tietoturvaratkaisut kuitenkin toimivat. Monet tietoturvaratkaisut ovat helppokäyttöisiä ja jokaiselle saatavilla olevia.

Avainsanat	matkustaminen, tietoturva, Tails

Metropolia

Author Title Number of Pages Date	Jani Tenhivaara Travelers information security package 38 pages 20 April 2018
Degree	Bachelor of Engineering
Degree Programme	Information and Communication Technology
Instructors	Head of Department Janne Salonen

The purpose of this thesis is to research different information security threats for travelers and how to prepare for them. Currently the use of information technology and trust for this technology is increasing, but information technology crime is also growing. Traditionally information security means information's availability, confidentiality and integrity. Nowadays non-repudiation and authentication are also attached to information security.

This thesis is divided into four parts. In first part I go through what different common threats there are for travelers. In second part how to avoid falling for these threats. In third part I bring up different security practices and programs and their qualities. In the last part I create step-by-step plan to how to improve information security in computers and phones, how to create protected Ubuntu OS and how to install security-focused operation system, Tails, for USB-memorystick.

Travelers should protect their own information before they are abroad, but also during and after their travel. Attackers can be non-governmental and different governmental agencies. According to Snowdens revelations, governmental agencies can be information security risks even indirectly, because they are weakening encryption protocols. Nevertheless widely and correctly done security measures still works. Most of security measures are easy to use and available for everyone.

Keywords	travelling, information security, Tails

Metropolia

Sisällys

Lyhenteet

Wi-Fi	Wi-Fi tai WiFi on teknologia langattomalle lähiverkolle.
WEP	Wired Equivalent Privacy on langattoman tietoliikenteen salausprotokolla.
WPA	Wi-Fi Protected Access on langattoman tietoliikenteen salausprotokolla.
RFID	Radio frequency identification, eli radiotaajuinen etätunnistus, on käytäntö tiedon etälukuun käyttäen RFID-tunnisteita.
NFC	Near Field Communication on RFID-tekniikka käyttävä kommunikointi protokolla. NFC-laite voi toimia sekä lukijana että tunnisteena.
DNS	Domain Name Server on järjestelmä, jolla muunnetaan verkkotunnuksia IP-osoitteiksi.
SSL	Secure Sockerts Layer on vanhempi salausprotokolla.
TLS	Transport Layer Security on salausprotokolla.
IMEI	International Mobile Equipment Identity on uniikki matkapuhelimen laite-tunnus, jolla tunnistetaan matkapuhelin verkosta.
VPN	Virtual Private Network on tapa liittää kaksi, tai useampi, verkkoa toisiinsa muodostaen näiden välille yksityisen verkon.
CVE	Common Vulnerabilities and Exposures on systeemi, jolla nopeasti voi tarkistaa tunnetut tietoturvahaavoittuvuudet.
EFS	Encrypting File System on Windowsin salausohjelma.
ZRTP	Z Real-time Transport Protocol on salaamisessa avainten vaihtoprotokol-la.

1 Johdanto

Insinöörityön tarkoituksena on tutkia matkailijoille aiheutuvia tietoturvauhkia ja miten näihin uhkiin voi varautua. Tietotekniikan kehittyessä lisääntyy matkailijan sähköisen tiedon määrä ja näin myös uhkien määrä, joten matkailijan pitää varautua oman tietoturvan ylläpitämiseen yhä enemmän. Osa tietoturvaratkaisuista on fyysisiä ja osa digitaalisia. Suurin osa tietoturvauhista on jokaisessa määränpäässä sama, joten samanlainen valmistautuminen riittää pitkälti. Omalla maalaisjärjellä matkailija pystyy myös ennakoimaan ja estämään osan tietoturvauhista.

Insinöörityö jakaantuu neljään osaan. Ensimmäisessä osassa muodostetaan kuva eri tietoturvauhkista ja -riskeistä matkailijoille. Osassa käydään läpi useimpia tyypillisiä tietoturvauhkia elektronisille laitteille.

Toisessa osassa perehdytään miten matkailija voi välttää näitä tietoturvauhkia. Osassa kootaan tietoa siitä, miten matkailija voi varautua tietoturvauhkiin ennen matkalle lähtöä, miten varautua matkalla ja mitä tehdä matkan jälkeen. Osassa käsitellään niin matkapuhelimen kuin tietokoneen varautumisia.

Kolmannessa osassa vertaillaan eri tietoturvallisuus vaihtoehtoja matkailijoille. Osan tarkoitus on tuoda esille useita eri tietoturvallisuuteen liittyviä ohjelmia, ratkaisuja ja käytäntöjä matkapuhelimille ja tietokoneille, vertailla näitä ja antaa matkailijalle hyvä kuva hänellä olevista vaihtoehdoista.

Työn loppuosa esittelee, miten matkailija itse voi vaiheittain parantaa tietoturvallisuuttaan, niin tietokoneilla ja puhelimilla. Käyn myös läpi miten uusi käyttöjärjestelmä asennetaan USB-muistitikulle ja miten tämä suojataan.

2 Tietoturvan ymmärtäminen

Tietoturva, eli tietoturvallisuus, on yleistermi, jolla perinteisesti tarkoitetaan tapaa ylläpitää tiedon luotettavuutta, eheyttä ja saatavuutta. Nykyään tietoturvallisuuteen liitetään myös todentaminen ja kiistämättömyys. Tieto voi esiintyä useassa eri muodossa, kuten digitaalisissa ja fyysisissä tallenteissa ja ihmisen omassa tietämyksessä. [1; 2 s. 20.]

Tiedon luotettavuudella tarkoitetaan tiedon salaisuuden ylläpitämistä ja tiedon luvattoman käsittelyn estämistä. Matkailijoille tämä ilmenee etenkin tiedon salaamisena ja tiedon hävityksenä. [1.]

Eheydellä tarkoitetaan tiedon luvattoman muutoksen estämisen ylläpitämistä tai muutos on havaittavissa. Tämä tarkoittaa, että vain valtuutetuilla on lupa muuttaa tietoa eikä tieto korruptoidu. Eheydellä voidaan myös tarkoittaa tietojen paikkansapitävyyttä ja loogisuutta. [1.]

Saatavuudella pyritään ylläpitämään tiedon olevan saatavilla, kun valtuutetut henkilöt tarvitsevat kyseistä tietoa. Tämä tulee esille varmuuskopioinnissa ja suojautumalla haittaohjelmilta ja verkkohyökkäyksiltä. [1.]

Todentamisessa tarkistetaan käyttäjän identiteetti ja hänen oikeutensa ennen tietoon tai systeemiin pääsyä. Tyypillisesti tämä toteutuu tunnus- ja salasanayhdistelmällä. [2 s. 22–23.]

Tietotekniikassa kiistämättömyydellä pyritään väärin käytön estämiseksi ja vähentämiseksi siihen, ettei tiedon siirrossa kumpikaan osapuoli voi kiistää tiedon siirtoon osallistumista. Henkilö ei voi kiistää lähettäneensä tai vastaanottaneensa tietoa. Sähköisessä tiedonsiirrossa tätä ylläpidetään esimerkiksi digitaalisilla allekirjoituksilla. [2 s. 23.]

3 Tietoturvauhat

Useimmat tietoturvauhista ovat jokaisessa maassa samat: matkailija voi tulla ryöstetyksi, laitteeseen voi tulla haittaohjelmia, laite voi joutua hyökkäyksen alaiseksi tai tiedon siirron luotettavuutta rikotaan. Matkailijan tietoturvaa voi myös rikkoa hallitusten osas-

tot. 2013 entinen NSA:n työntekijä Edward Snowden paljasti NSA:n ja tämän kumppaneiden maailmanlaajuisia joukkovalvontaan liittyviä menetelmiä ja asiakirjoja. Snowdenin paljastuksista kävi ilmi, että tiedustelujärjestöt ovat tiedonkeruun lisäksi muun muassa piilottaneet takaovia salausohjelmiin heikentäen ohjelmien turvallisuutta kaikille ja heikentäneet kansainvälisiä salaukseen liittyviä standardeja [3]. Osa tiedustelujärjestöistä on muodostanut tiedusteluliiton, Five Eyesin [4], jonka järjestöt voivat kiertää kotimaan kansalaisten tiedonkeruuseen liittyviä rajoituksia ja lakeja tarjoamalla toisilleen toisten kansalaisista keräämäänsä tietoa [5]. Tietoturvauhkia lisää tiedusteluvirastojen tekemät hakkerointiohjelmat ja näiden ohjelmien leviäminen. Wikileaks väitti 2017, että CIA menetti hallinnan suuresta osasta heidän hakkerointikalustoastaan [6]. Näiden joutuminen julkiseen käyttöön lisää matkailijan tietoturvauhkia.

Suurin osa internetin käyttäjistä käyttää myös sosiaalista mediaa, kuten Facebookia, Twitteriä ja Instagramia [7]. Osassa sosiaalisesta mediasta on kuitenkin isoja tietoturvauhkia yksityiselle tiedolle. 2018 tuli ilmi, että jopa 87 miljoonan Facebookin käyttäjän tietoturvallisuus rikkoutui ja konsulttiyhtiö Cambridge Analytica pääsi käsiksi heidän tietoihinsa. Iso-Britannialainen uutisyritys The Week myös raportoi, että Cambridge Analytican toimitusjohtaja myönsi heidän käyttäneensä tietoja poliittisiin tarkoituksiin [8]. Facebook on myöntänyt tutkivansa käyttäjiensä lähettämiä linkkejä, kuvia ja Messenger-viestejä [9].

Osa tietoturvauhista voi olla väistämättömiä, etenkin eri valtioiden lait. Useassa maassa rajojen ylityksen aikana viranomaisilla on laillinen oikeus takavarikoida epäilyttävät laitteet ja esimerkiksi Yhdysvaltojen hallitus tiedottaa kansalaisilleen, että Israelin rajaviranomaiset ovat sisäänpääsyn ehtona pyytäneet pääsyä matkailijan henkilökohtaiseen sähköpostipalveluun [10]. Kiinassa puolestaan tuli 2015 voimaan antiterrorismilaki, jonka takia teknologia yritykset joutuvat luovuttamaan salausavaimet. Salausavaimilla Kiinan hallinto pystyy helposti purkamaan varastoimansa salatut tiedot, oli tieto sitten viesti tai tiedosto [11]. Vanhempi insinööri Stuart Barton kertoo, että poistuessaan Armeniasta viranomaiset halusivat Stuartin todistavansa omistaneensa jo kannettavan tietokoneensa ennen maahan tuloa. Stuart joutui käynnistämään kannettavansa ja näyttämään muista maista ottamiaan kuvia, jotta viranomaiset uskoivat häntä [12].

Lähivuosina on myös tullut esille valetukiasemia. Valetukiasemat imitoivat oikeita tukiasemia ja yrittävät saada matkapuhelimet yhdistymään itseensä. Valetukiasemat myös kopioivat puhelimesta ESN-numeron, IMSI-numeron ja muuta metadataa. Meta-

datan avulla valetukiasema voi lähettää puhelimeen valeviestejä ja -puheluita [13]. Välillä valetukiasemia eivät käytä vain siviilihenkilöt, mutta jopa hallitusten osastot laittomasti. Yhdysvalloissa poliisit ovat käyttäneet valetukiasemia ilman valtuuksia, jolloin sivullisten metadataa on vuotanut. Teoriassa valetukiasemia ei pysty tunnistamaan oikeista [14].

Määränpäässään matkailijalla on mahdollisuus käyttää julkisia Wi-Fi-yhteyksiä ja terminaaleja. Ongelmana on kuitenkin näiden turvallisuus. Nortonin 2013 julkaistaman raportin mukaan jopa 68 % julkisten ja suojaamattomien Wi-Fi-verkkojen käyttäjistä joutuu kyberrikosten uhriksi [15]. Ilmaisissa julkisissa Wi-Fi-verkoissa on monia syitä, jotka tekevät niistä tietoturvauhan. Osa vanhemmista langattomista verkoista käyttää vanhempia standardeja salaamiselle, kuten WEP ja WPA, joista on löydetty heikkouksia, tai ei käytä salaamista ollenkaan. Toinen uhka on rikollisten luomat Wi-Fi-yhteydet, joissa hyökkääjä käyttää mies välissä -hyökkäystä. Onnistuneella hyökkäyksellä rikollinen voi siepata siirrettävää tietoa ja lukea ja muokata tietoa. Julkisissa terminaaleissa on riskinä, että tietokoneessa on valmiiksi haittaohjelmia, jotka vakoilevat ja tallentavat käyttämääsi tietoa, ja joku voi seurata käyttäjän takaa fyysisesti näytöllä olevaa tietoa. [16.]

RFID-tunnusta käyttävien tavaroiden, esimerkiksi lähimaksukorttien, passien ja puhelimien NFC -tekniikan määrä on kasvanut ja samalla on kasvanut huoli siitä, että rikolliset pääsevät lukemaan tavaran tiedot omilla laitteillaan. Tekniikan Maailma testasi 2017 RFID-tunnuksen lukuhelppoutta ja heidän testissään kävi ilmi, että rikollinen voi tehokkaalla radiolaitteella lukea tietoja suoraan taskussa tai käsilaukussa olevasta pankkikortista [17]. Toisaalta Finanssivalvonnan mukaan RFID-tunnusteita käyttävissä lähimaksukorteissa ei ole vielä 2017 mennessä ollut väärinkäytöksiä. Molempien Finanssivalvonnan [18] ja kolumnisti Roger Grimesin mukaan RFID-tunnusteita käyttävään rikollisuuteen ei ole huolta:

> ...not a single crime involving an RFID-enabled device has been reported in the public domain. [19]

2017 tapahtuneen Mercedes-Benzin auton varastamista on väitetty RFID-rikokseksi, mutta Grimesin mukaan ei ole todisteita, että rikoksessa olisi käytetty RFID:n langatonta teknologiaa [20].

Laitteita valittaessa tulee myös kiinnittää huomiota käyttöjärjestelmään ja kerääkö se tietoa käyttäjästä. 2017 tuli ilmi, että kiinalainen älypuhelinvalmistaja OnePlus keräsi käyttäjiltään salaa laitetietoa ja käyttötietoa [21]. Windows 10 puolestaan kerää perusoletuksena käyttäjältä tietoa, kuten sijainnin, äänikomentoja ja Microsoftin verkkoselainten tietoja [22]. Käyttäjä voi Windows 10:ssä poistaa päältä tiedonkeruuasetuksia, mutta käyttöjärjestelmä silti kerää Basic-tason tietoa. Tämä tarkoittaa, mitä Microsoftin mukaan on kriittistä ymmärtää laite ja laitteen kokoonpano [23].

Verkkoselain on usein ensimmäinen yhteys verkkoon, joten selaimen suojaaminen on tärkeää. Verkkoselaimet ovat suosituimpia ohjelmia laitteilla, joten ne ovat suosittuja kohteita haittaohjelmien tekijöille. Haittaohjelmien lisäksi mainostajat ja itse sivut voivat seurata käyttäjää. Yleisimmät verkkoselainhyökkäykset kohdentuvat selaimessa oleviin haavoittuvuuksiin, kolmannen osapuolen liitännäisissä oleviin haavoittuvuuksiin ja verkkosivuille ohjaaviin DNS-palvelimiin. Verkkopalvelut usein tallentavat käyttäjälle evästeitä, joilla tallennetaan muistiin käyttäjän tekoja ja tietoja. Hyökkäämällä evästeisiin hyökkääjä voi saada tietoa käyttäjästä tai hyökkääjä voi huijata verkkoselaimen tekemään jotain ilkeää käyttäjän puolesta. [24; 25.]

4 Tietoturvauhkien välttäminen

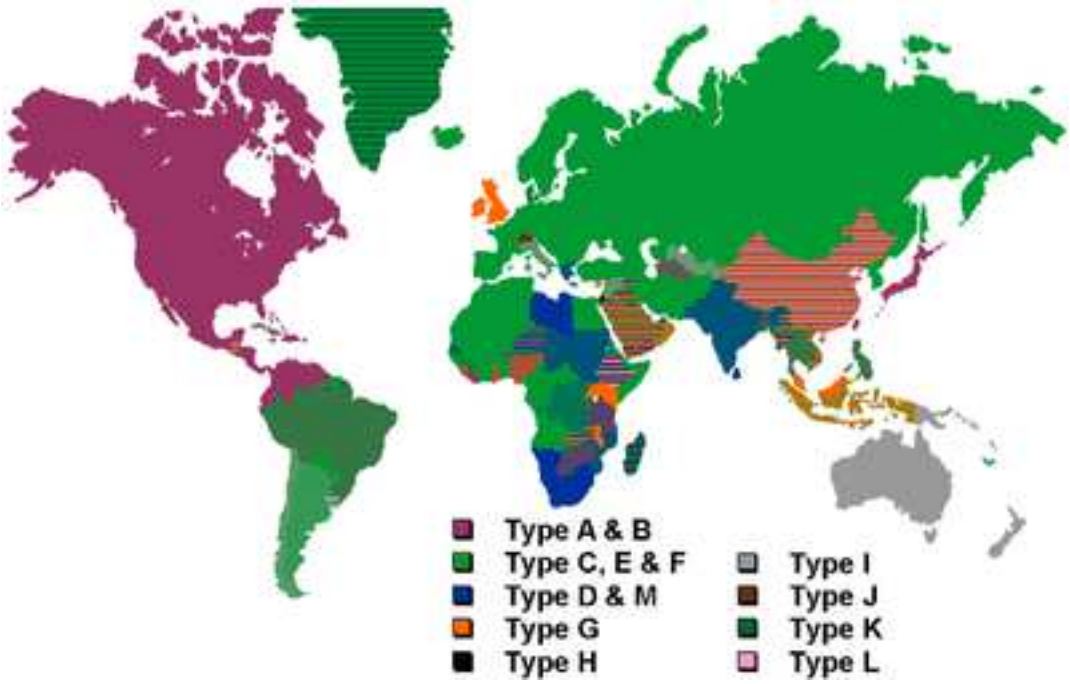
4.1 Uhkien välttäminen ennen matkalle lähtöä

Ylläpitääkseen omaa tietoturvaansa matkailijan pitää aloittaa varautuminen jo ennen matkalle lähtöä. Tärkeää on myös, että matkailija kokeilee tietoturvaratkaisujensa toimivan, jottei huomaa kesken matkansa näiden toimimattomuuden. Useimmat tietoturvauhkiin varautumiskeinoista ovat yksinkertaisia, kuten ohjelmien päivittäminen, salasanojen asentaminen, varmuuskopioiden ottaminen, palomuurin ja virustentorjuntaohjelmien tarkistaminen ja mahdollinen asentaminen, ylimääräisten tietojen poistaminen laitteista ja muiden tarvittavien tietoturvaohjelmien asentaminen. Valitsemalla omaa tietoturvallisuutta lisääviä ohjelmia, matkailijan pitää ottaa huomioon itse ohjelman turvallisuus. Ohjelma voi olla huono, haittaohjelma tai se kerää tietoa käyttäjältä. Välttääkseen huonot ohjelmat matkailijan tulee itse tutkia valitsemansa ohjelman luotettavuus, koska ohjelmien luotettavuus voi muuttua ajan myötä.

Matkailija voi myös ottaa käyttöön vanhemman laitteen tai lainata töistään lainalaitteen. Näissä on yleensä vähemmän tietoa, mutta omien vanhojen laitteiden muisti kannattaa tarkistaa ja tyhjentää ylimääräisestä tiedosta. Matkustaja voi kuitenkin hankkia uuden laitteen, joka on tarkoituksella rakennettu turvalliseksi. Saksalainen yritys GSMK tekee ja myy salattuja puhelimia, joissa he markkinoivat olevan valmiiksi salattu viestintä, soittaminen ja tieto. [26.]

Lisätäkseen tietoturvaansa matkailija voi myös hankkia muita fyysisiä tietoturvallisuutta lisääviä apuvälineitä. Lompakon ja repun voi suojata RFID-lukijoilta erillisillä suojalompakoilla ja -repuilla. Matkailija voi myös itse rakentaa oman RFID-suojan käärimällä RFID-tunnusta käyttävän tavaran tai laitteen alumiinifolioon rakentaen näin Faradayn häkin [19]. Omniscience is a bliss -verkkoartikkelin mukaan alumiinifolio ei kuitenkaan kokonaan eristä RFID-tunnusta, mutta siitä on apua estämään kaukaa lukemisen [27]. Toinen tietoturvallisuutta lisäävä tavara on näytön päälle asetettava suoja, jonka avulla näyttö näkyy vain tietystä kulmasta. Tällöin ulkopuoliset eivät näe fyysisesti käyttäjän takaa näytöllä olevaa tietoa.

Tiedon saatavuuden varmistamisen kannalta matkailijan on suositeltava kantaa mukanaan varavirtalähdettä ja määränpäähän sopivaa adapteria verkkojohdolle. Euroopan ulkopuolella, ja jopa sisäpuolella (kuva 1), sähköverkkojärjestelmien pistokkeet ja verkkovirta voivat olla erilaisia kuin Suomessa. Esimerkiksi Iso-Britanniassa on käytössä sama verkkovirta kuin Suomessa, mutta eri tyypin pistoke: G-tyyppi.



Kuva 1. Pistoketyyppien jakautuminen maailmalla. [28.]

Seuraavana matkailija voi ottaa käyttöön matkan ajaksi uuden sähköpostitilin tai tarkistaa jo olemassa olevan tietoturvasuojan. Suojatakseen hyödyllisesti sähköpostin, pitää salata kolme asiaa: yhteys sähköpostia tarjoavalle, itse viesti ja viestin varastointi. Matkailijan pitää myös miettiä, ketä vasten haluaa suojautua. Jos matkailija haluaa paremman tietoturvasuojan Yhdysvaltojen hallitusta vastaan, niin hänen kannattaa silloin hankkia Yhdysvaltojen ulkopuolella oleva sähköpostipalvelin. Suojatakseen internetselaimen kautta yhteyden sähköpostipalvelimelle, osa sähköpostitarjoajista tarjoaa SSL/TLS-salausta käyttäviä sivuja. Tämä näkyy, kun sivun osoitteessa on HTTP:n sijaan HTTPS. Sähköpostiohjelmissa voi myös asetuksista tarkistaa, onko mahdollista laittaa salaus päälle. Suojatakseen itse viestin, osa tarjoajista antaa mahdollisuuden suojata viesti, mutta matkustaja voi asentaa ulkopuolisen salausohjelman. Tällöin joutuu kuitenkin luottamaan kolmannen osapuolen turvallisuuteen. Laitteelle tallennetut viestit pystyy suojaamaan salaamalla itse laiteen kovalevyn.

Käytetään kaksivaiheista tunnistautumista, jos tämä on mahdollista. Tämän tarkoituksena on todentaa henkilöllisyys kahden eri tunnistautumismenetelmän kautta, jolloin rikollinen ei pääse tietoihin käsiksi varastamalla vain toisen tunnistautumismenetelmän tiedot. Riskinä on kadottaa toinen tunnistautumismenetelmä, kuten USB-muistilaite tai puhelin, jolloin palveluun pääseminen estyy. Yhdysvaltojen Valkoinen talo julkaisi 2016 tiedotteen, jossa kyberturvallisuuden kannalta suositellaan käyttämään useamman tunnistautumismenetelmän käyttämistä verkkopalveluihin sisäänkirjautuessa [29].

Kannattaa tutkia oman pankin käytäntö ulkomailla. Toimiiko kortti määränpäässä ja onko kortissa maarajoituksia? Pankkikorteissa voi olla tietoturvaratkaisuna ulkomaisen käytön tarkkailu ja automaattinen tilin lukitus epäilyttävän käytön takia. Pankit voivat myös tarjota maarajoituksia, esimerkiksi Danske Bank ja Ålandsbanken, joilla matkusta voi sallia kortin käytön vain tietyille alueille [30]. Tietyissä pankeissa tietoturvan takia matkailijan pitää ilmoittaa ennen matkastaan ja sallia kortin käyttö määränpäässään. Tässä uhkana osa pankeista rajoittaa sallittavien maiden määrää matkalle [31]. Matkustajan on tällöin kannattavaa ottaa käteistä rahaa mukaansa. Verkkoasioinnissa tietoturvauhat ovat samat kuin muulle verkkotoiminnalle, joten matkustajan varautuminen tähän on samanlaista kuin muuhun verkossa asiointiin.

Laitteiden muistin salaaminen on yksi tietoturvan perusratkaisuista. Kovalevyn salaamisella varmistetaan, että vaikka laite tai tiedot varastettaisiin, niin tieto pysyy salassa. NSA:n ilmiantaja Edward Snowdenin mukaan asianmukaisesti tehty salaaminen on yksi ainoista asioista, johon voi luottaa [32]. Matkustaja voi myös salata vain tietyn osuuden laitteen muistista, joka on helpompaa kuin koko kovalevyn salaaminen, mutta ei yhtä tietoturvallista. Useat tietokoneiden ja älykännyköiden käyttöjärjestelmistä tarjoavat valmiiksi laitteella tietojen salaamista.

Verkosta on myös saatavilla ilmaisia salausohjelmia, mutta näissä käyttäjän pitää luottaa ohjelman tarjoajaan. Salausohjelma voi sisältää haittaohjelman tai takaoven. Töistä saatavilla laitteilla voi olla jo salausohjelma käytössä ja työpaikalla voi olla omat käytännöt salaukseen, joten matkustajan tulee itse tarkistaa tämä.

Henkilön todentaminen tapahtuu useimmiten salasanoilla, joten vahvan salasanan valitseminen on tärkeää tietoturvalle. Mitä vahvempi salasana, niin sitä kauemmin väsytyshyökkäyksellä salasanan arvaaminen kestää. Vahvana salasanana pidetään pitkää ja mahdollisimman monimutkaista salasanaa. Monilla verkkopalveluilla on omat minimivaatimukset hyväksyttäville salasanoilla. Kuten Googlella salasanan pitää olla ainakin 8 merkkiä ja sisältää isoja ja pieniä kirjaimia [33]. US-CERT puolestaan neuvoo, että etenkin ollakseen hyvä salasana salasanan tulisi olla niin pitkä kuin mahdollista ja välttävän sanoja, joita löytää sanakirjasta. Salasanan ollessa vahva, sen pitäisi myös olla eri jokaiselle tunnuksellesi. Tällöin, vaikka yhdestä ohjelmasta vuotaisi salasana, niin tietoturva pysyy ennallaan toisille tunnuksille. Monien vahvojen salasanojen muistaminen voi kuitenkin olla haastavaa, joten on mahdollista hankkia salasanamanageri, johon tallentaa salasanat. [34.]

Verkkoselaimen turvallisuutta matkailija voi parantaa nopeasti ja helposti. Verkkoselaimen päivittämisen lisäksi matkailija voi asentaa turvallisuutta lisääviä liitännäisiä ja poistaa turhia liitännäisiä. Suositut verkkoselaimet, Firefox ja Chrome, tarjoavat omissa suojausasetuksissa myös muutamia vaihtoehtoja, joilla matkailija voi lisätä tietoturvaansa, kuten estämällä historian keräämisen laittamalla Do Not Trackin päälle, estämällä salasanojen muistamisen ja antamalla verkkoselaimen estää vaarallisen sisällön. Matkailija voi myös käyttää suoraan selaimen yksityisen selaamisen, joka oletuksena ei tallenna selaimen muistiin käytyjä sivuja, tilapäistiedostoja ja evästeitä. Verkossa käymisen yksityisyyden lisäämistä varten matkailija voi ladata Torin. Tor-palvelun tarkoituksena on pysyä tuntemattomana internetselailun aikana. Torilla on kuitenkin omia ongelmia ja riskejä. NSAn on raportoitu kohdistavan hyökkäyksiä Torin käyttäjille ja Toria käyttävät voidaan tunnistaa alle kuudessa kuukaudessa. [35; 36.]

Fyysisten tietojen häviämiseen matkailija voi varautua ottamalla varmuuskopioita elektronisiin laitteisiinsa. Pankit voivat tarjota varakortteja, jolloin toisen kortin katoamisessa ei joudu pulaan [30]. Jos matkustajan fyysinen tavara varastetaan, niin tietoturvan ylläpitämiseksi matkustajan tulee ilmoittaa varkaudesta asianmukaisille henkilöille, esimerkiksi pankkikortin katoamisesta ilmoittaa pankille, jolloin varkaat eivät pääse käyttämään tietoja hyväkseen.

4.1.1 Puhelimen suojaaminen

Ensimmäisenä matkailijan kannattaa varautua matkapuhelimen hävittämiseen tai varkauteen joutumiseen. Tätä varten matkapuhelimissa on oma uniikki IMEI-numerosarja, jonka saa näyttöön näkyville avaamalla soittamissovelluksen ja näppäilemällä *#06#. Seuraavana matkailijan kannattaa ottaa käyttöön etähallintaominaisuus, jonka kautta matkailija voi lukita, vaihtaa salasanan ja pyyhkiä kännykässä olevat tiedot. Android-puhelimilla on käytössä Googlen Android Device Manager -verkkosivu, jonka kautta Android-puhelimien etähallinta onnistuu.

Matkailijan on suositeltavaa myös ottaa käyttöön näytönlukitus. Tämä on perinteisesti neljän numeron PIN-koodi. Uudemmat älypuhelimet tarjoavat myös pidempää PIN-koodia, aakkosellista salasanaa, kuviokoodia, sormenjälkitunnistinta ja kasvojen tunnistusta puhelimen avaamiseen. Kasvojen tunnistus on kuitenkin raportoitu olevan epäluotettava, joten matkailijan on käyttää muuta menetelmää näytönlukitukseen. Tietotur-

va-asiantuntija Leigh-Anne Galloway väittää biotunnistautumisen olevan liian erehtyväinen ja suosittelee käyttämään pitkää satunnaisesti luotua salasanaa [37].

Muita tietoturvaratkaisuja on poistaa tai kytkeä pois päältä turhat ohjelmat. Vanhoissa ohjelmissa voi olla päivittämättömiä tietoturva-aukkoja, ja ohjelma on voinut tallentaa ylimääräistä tietoa käyttäjästä. Kannattaa asettaa puhelimensa käyttämään uudempaa 3G-verkkoa. Uudemmissa verkoissa on paremmat salaukset verrattuna 2G-verkkoon [38]. Kytke Wi-Fi, Bluetooth ja NFC pois päältä, jos näitä ei ole tarve käyttää. Etenkin Bluetoothilla on ollut haavoittuvuuksia, kuten Armis IoT -turvallisuusyrityksen löytämä haavoittuvuuskokoilma BlueBorne, jolla hyökkääjä pystyy ottamaan laitteen kokonaan hallintaansa [39].

Muistin lisäksi kommunikointi voidaan salata. Valmiiksi salattujen puhelimien lisäksi puhelimiin on tarjolla ilmaisia salausohjelmia, kuten Signal, jotka käyttävät päästä päähän -salaamista suojatakseen kommunikoinnin. Valittaessa kommunikointiohjelmaa matkustajan tulee myös tarkistaa, toimiiko ohjelma määränpäässä ja kerääkö itse ohjelma laitteesta tietoa. Facebookin omistaman viestintäohjelma Messengerin, joka tarjoaa päästä päähän -salausta, on raportoitu keränneen käyttäjän metadataa [40].

4.1.2 Tietokoneiden suojaaminen

Tietokoneiden tietoturvan parantaminen on pitkälti samanlainen kuin matkapuhelimen. Matkailijan tulee päivittää ohjelmat, asentaa ja kytkeä päälle haittaohjelmia torjuvat ohjelmat, asentaa salasanat ja poistaa ylimääräinen tieto laitteesta. Tietokoneilla BIOS latautuu ennen käyttöjärjestelmää, joten BIOS:iin suuntautuva haittaohjelma voi toimia ennen käyttöjärjestelmän turvaohjelmia. Perusturvaa BIOS:iin tarjoaa BIOS-salasana, jolla matkustaja voi estää luvattoman pääsyn. Matkailijan tulee ottaa huomioon paljonko hän tarvitsee laitteeseen oikeuksia ja onko tarpeen käyttää järjestelmävalvojatunnusta, vai voiko hän luoda ja käyttää normaalikäyttäjän tunnusta.

Ulkoisilta muistilaitteilta voidaan käynnistää tietokoneen hakkerointiin tarkoitettuja ohjelmia ja käyttöjärjestelmiä. Tätä varten on tärkeää estää ulkoisilta muistilaitteilta käynnistäminen BIOS:in asetuksista.

4.1.3 Ulkoiset muistilaitteet ja digitaaliset laitteet

Ulkoisten muistilaitteiden turvaaminen tapahtuu suurimmaksi osaksi samalla tavalla kuin muidenkin laitteiden. Matkailijan tulee pitää silmällä laitteitaan varkaiden varalta ja osalle ulkoisista muistilaitteista pystyy asentamaan salaamisohjelman. Matkailija voi myös hankkia valmiiksi salatun muistilaitteen, jossa voi olla salausohjelma jo asennettu tai itse laitteessa on näppäimistö, jonka kautta annetaan PIN-koodi.

Kameravalmistajia on pyydetty rakentamaan itse laitteeseen salausmenetelmä, mutta ZDNetin tekemän artikkelin mukaan kameravalmistajat vastustavat tätä. Tällä hetkellä turvallisinta on siirtää mahdollisimman nopeasti kameran tieto muille laitteille. Kameran muistina olevalle SD-kortille on kehitteillä salausohjelmia, jotka salaavat datan samalla, kun kamera kuvaa. Canonin kameroihin keskittyvä Magic Lantern on yksi salausohjelmista, mutta tämä on vielä kehittämisvaiheessa ja vaatii kameran laiteohjelmiston muuttamista. [41; 42.]

4.2 Uhkien välttäminen matkalla

Normaalilla maalaisjärjellä pystyy välttämään useimpia tietoturvauhkia matkalla. Perustietoturvaratkaisuja on laitteiden sammuttaminen, kun niitä ei käytetä, pitämällä laitteita silmällä varkaiden varalta, ei käytä tuntemattomia ulkoisia muistilaitteita, käyttää vain tunnettuja ja luotettuja Wi-Fi:jä, eikä kirjaudu sisään julkisilla terminaaleilla. Osan näistä uhkista voi välttää toisille tietoturvaratkaisulla, kuten VPN-palveluilla.

VPN-palvelun tarkoituksena on salata käyttäjän verkkoliikenne VPN-palveluntarjoavalle saakka ja salata käyttäjän oma sijainti ja IP-osoite. Tarkkailemalla liikennettä ulkopuolinen näkee liikenteen menevän palveluntarjoajalle. Matkailijalle hyötynä VPN-palvelu antaa pääsyn valvonta- ja sensuuriohjelmien ohitse, kuten esimerkiksi Kiinan suuren palomuurin kiertäminen. VPN-palvelun avulla matkustaja voi myös käyttää turvallisemmin julkisia wlan-verkkoja, koska verkkoasiointi on salattu. Ennen matkalle lähtöä on kuitenkin suositeltavaa tarkistaa, onko VPN-palveluiden käyttö määränpäässä laillista ja onko kohdemaa vain estänyt valitun VPN-palvelun käytön. Kiinassa osa suosituista VPN-palveluista on estetty. Venäjällä, Kiinassa ja osin Lähi-idässä VPN-palveluiden käyttöä on rajoitettu kieltämällä VPN-palveluita tarjoavia nettisivuja ja julistamalla vain hallituksen sallimat VPN-palvelut laillisiksi. NSA:n on raportoitu harjoittavan laajamittaista VPN-palveluiden hyväksikäyttöä ja sieppaavan siirrettävän tiedon. [43; 44.]

Tietojen tallentamiseen matkailijan tulee salata käyttämänsä laitteen muisti. Matkailija voi myös käyttää pilvipalveluita, jolloin laitteen häviäminen ei kadota tietoja ja matkailija pystyy myös jakamaan tietojansa toisten kanssa paremmin. Lähivuosina on tullut esille muutamia pilvipalveluiden vuotoja, kuten 2014 iCloud vuosi melkein 500 yksityistä kuvaa ja 2012 Dropboxista hakkeroitiin 68 miljoonan käyttäjän tietoja [45; 46]. Tästä huolimatta osa asiantuntijoista pitää pilvipalveluita turvallisempana verrattuna perinteisiin IT-systeemeihin. Pilvipalveluasiantuntija ja analyytikko David Lintihicum kertoo pilvipalveluiden turvallisuudesta:

> Yleisesti puhuen, olen löytänyt pilvipalveiden olevan turvallisempia verrattuna perinteisiin systeemeihin. [47]

Pilvipalveluita käyttäessä tieto on vaarassa vuotaa kahdella eri tavalla, kun sitä siirretään ja kun tieto on varastoitu pilvipalveluun. Tätä varten tallennettava tieto tulisi jo ennen siirtoa olla salattu, kuten AxCrypt-salausohjelmalla tai käyttämällä pilvipalvelua, joka tarjoaa päästä päähän -salaamisen.

4.3 Uhkien välttäminen matkan jälkeen

Jotta matkailijan tietoturva säilyy matkan jälkeenkin, on hänen vielä suoritettava muutamia toimenpiteitä. Matkailijan on suositeltavaa vaihtaa salasanansa, tarkistaa laitteet haittaohjelmien varalta ja tarkkailla pankkitilinsä tietoja mahdollisten vuotojen vuoksi. Jos jokin laitteista on saastunut, niin on suositeltavaa tyhjentää laite ja mahdollisesti formatoida se uudestaan. Työasioissa matkaavan henkilön kannattaa myös raportoida mahdollisista tietoturvallisuuden liittyvistä tapahtumista työnantajansa IT-osastolle.

5 Matkailijan tietoturvavaihtoehdot ja näiden vertaileminen

5.1 Käyttöjärjestelmien tietoturvallisuus

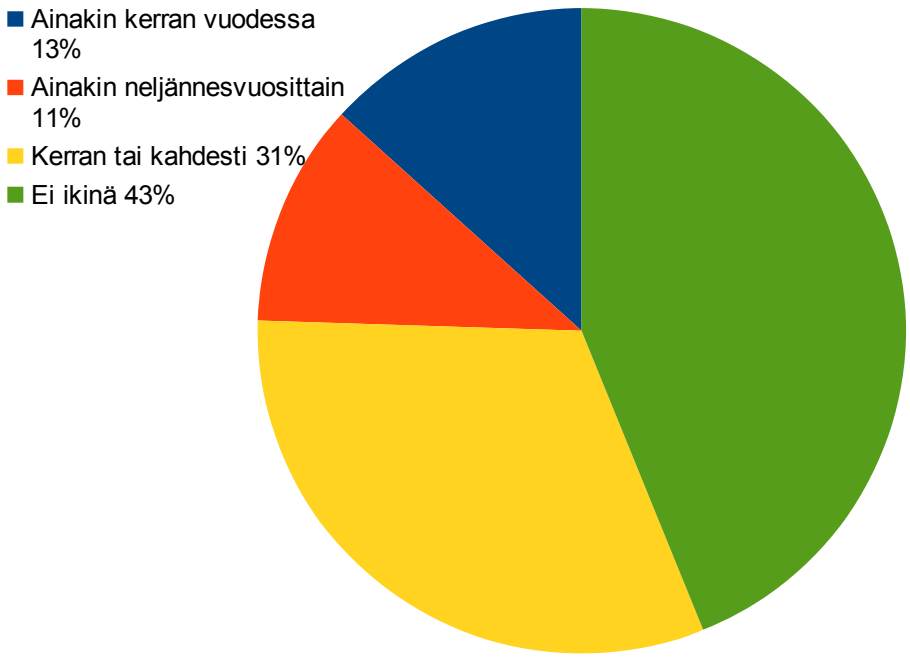
Mikään käyttöjärjestelmä ei ole täysin turvallinen. Eri käyttöjärjestelmissä on eri määrä haavoittuvuuksia. 2017 CVE Detailsin tekemän tilaston mukaan eniten haavoittuvaisuuksia oli Androidilla, ja tämän jälkeen pienentyvässä järjestyksessä iOS, Mac OS X ja Windows 10 [48]. Jos matkustaja pystyy valitsemaan käyttöjärjestelmänsä, niin omien tarpeiden lisäksi kannattaa ottaa huomiota muutama asia: milloin käyttöjärjestelmä

julkaistiin ja kuinka suosittu käyttöjärjestelmä on. Vanhoja käyttö-järjestelmiä ei mahdollisesti enää päivitetä, jolloin näissä olevat tietoturva-aukot jäävät korjaamatta. Haittaohjelmien tekijät myös keskittyvät suosituille käyttöjärjestelmille, jotta mahdollisuudet uhreihin olisivat suuremmat. Matkustajalla ei aina ole kuitenkaan mahdollisuutta valita, mitä käyttöjärjestelmää käyttää, jolloin parhain tietoturvaratkaisu on tarkistaa käyttöjärjestelmän olevan päivitetty.

Tietokoneissa Windowsin käyttöjärjestelmät ovat suosituimpia Net MarketSharen ja StatCounterin mukaan tietokoneista yli 80 % käyttää Windows-käyttöjärjestelmiä [49; 50]. Suosionsa takia Windows-käyttöjärjestelmille on luotu enemmän haittaohjelmia muihin käyttöjärjestelmiin verrattuna [51]. Windowsilla on myös ollut historian aikana monia suuria tietoturvaongelmia. Uudessa Windows 10:ssä on muutamia ominaisuuksia tehdasoletuksena päällä, jotka ovat tietoturvauhkia, esimerkiksi Cortana, jonka on raportoitu olevan suuri tietoturvauhka [52].

MacOS X:ää usein kuvaillaan turvalliseksi vaihtoehdoksi. Mutta CVE:n haavoittuvuusraporttien mukaan näkee, että macOS X;ssä on myös haavoittuvuuksia olemassa. Axiom Cyber Solutionsin toimitusjohtaja Troy Wilkinsonin mukaan macOS X on Windowsta turvallisempi, mutta lisää, ettei se ole enää täysin turvallinen [53].

Linux-pohjaisia käyttöjärjestelmiä yleisesti pidetään turvallisempana vaihtoehtona Mac OS:ään ja Windowseihin verrattuna. Syinä on avoin lähdekoodi, jonka ansiosta kuka vain voi tarkistaa lähdekoodin takaovien ja bugien varalta, pienempi käyttäjämäärä ja eri ympäristöjen määrä [54]. Avoin lähdekoodi kuitenkin antaa myös haittaohjelmien tekijöille ja hakkerijoille mahdollisuuden tutkia lähdekoodia haittatarkoituksiin. Avoin lähdekoodi ei myöskään tarkoita suoraan, että aina useat henkilöt tutkisivat lähdekoodin turvallisuuden. Snykin 2017 tekemän tutkimuksen mukaan 43 % lähdekoodin ylläpitäjistä ei ole ikinä tutkinut omaa koodiansa (kuva 2). Snyk myös raportoi, että haavoittuvuuden löytymiseen kestää keskimäärin yli 2 vuotta ja löytymisen jälkeen korjaukseen kestää keskimäärin 16 päivää. [55]



Kuva 2. Kuinka usein ylläpitäjä on tarkastanut koodinsa. [55.]

Matkustajan tulee kuitenkin ottaa huomioon, että suositut macOS- ja Windows-ohjelmat eivät mahdollisesti toimi Linux -pohjaisissa käyttöjärjestelmissä. Keskivertomatkustaja voi myös huomata Linuxiin perustuvien käyttöjärjestelmien olevan hieman vaikeammin käytettäviä.

Linuxilla on myös monia tietoturvallisuutta varten rakennettuja käyttöjärjestelmiä, kuten Snowdenin suosittelema Qubes OS. Qubes OS pohjautuu Xen-virtuaalikoneeseen, joka keskittyy turvallisuuteen eristäytymisen kautta. Qubesissa oletetaan, ettei ole täydellisiä ohjelmia, ja yhden ohjelman haavoittuvuus voi rikkoa koko laitteen tietoturvan. Tätä varten Qubesissa voi eristää ohjelmat omiin ympäristöihin, jolloin haittaohjelma pääsee vain tietyn ympäristön sisällä olevaan tietoon käsiksi. Huonoina puolina Quabesissa eristäminen pitää tehdä manuaalisesti, eikä käyttöjärjestelmä toimi kaikissa laitteissa. [56; 57.]

Puhelimissa suosituimmat yhä kehittelyssä olevat käyttöjärjestelmät ovat Googlen Androidiin perustuvat käyttöjärjestelmät ja Applen iOS. Windows Phone oli kolmas suosittu käyttöjärjestelmä puhelimiin, mutta tämän kehitys lopetettiin 2017 [58]. Jokaisella käyttöjärjestelmällä on omat riskinsä. Android on avoimeen lähdekoodiin perustuva, mutta usein osa koodista on salattu. CVE Detailsin mukaan 2017 Androidilla oli yli kaksinkertainen määrä haavoittuvuuksia iOS:ään verrattuna ja Nortonin mukaan Androidiin koh-

distuu enemmän haittaohjelmia [48; 59]. Monet tietoturvauhista voi kuitenkin välttää päivittämällä käyttöjärjestelmänsä uusimpaan versioon [59]. IOSn tietoturvaa lisää Applen tiukka kontrolli käyttöjärjestelmästään ja päivitysten tullessa jokainen saa ne [60]. Monien älypuhelimien tietoturvallisuutta rikkoo myös hallituksen virastot. 2013 raportoitiin, että NSA- ja GCHQ-tiedusteluvirastot pystyvät lukemaan suuren osan yksityisistä tiedoista älypuhelimissa [61]. 2014 julkaistiin, että tiedusteluvirastot pystyvät kuuntelemaan puhelimessa olevien ohjelmien, esimerkiksi Angry Birdsin, verkkoliikennettä ja kopioimaan tästä tietoa [62].

5.2 Tietojen salaaminen

Useimmat laitteet tarjoavat valmiina omia salausohjelmia, esimerkiksi osalla Windows-käyttöjärjestelmistä on valmiina Bitlocker. Snowdenin paljastusten mukaan jotkut tietotekniikka yhtiöt, esimerkiksi Microsoft, ovat kuitenkin olleet yhteistyössä NSA:n kanssa kiertääkseen salauksia, esimerkiksi Outlook [3]. Tätä varten matkailijan tulee miettiä avoimeen lähdekoodiin perustuvia vaihtoehtoja. Matkailijan tulee myös ottaa huomiota itse laitteeseen, koska kovalevysalaus voi huomattavasti hidastaa laitetta, salauksen jälkeen tiedon palauttaminen vaikeutuu ja tarvitsee koko kovalevyn salaamista, vai riittääkö salaamiseen vain osuus. [63.]

Uudemmissa älypuhelimissa salaus voi olla jo tehdasasetuksena päällä. Salauksen voi käydä tarkistamassa asetuksista, kuten iPhoneilla tämä lukee Touch ID & Passcode asetuksen pohjalla ”Data protection is enabled.”. Android-puhelimilla salausasetukset riippuvat puhelimesta ja asetuksien sijainti voi olla suojausasetuksissa tai tallennustila-asetuksissa. Puhelimien omat salausohjelmat usein salaavat koko laitteen, joten jos matkailija haluaa salata vain osan, hänellä on myös vaihtoehtona hankkia kolmannen osapuolen salausohjelma. [64.]

Tietokoneilla on harvemmin valmiita salausohjelmia, joten matkailijan tulee itse tarkistaa ja mahdollisesti asentaa omat salausohjelmat. Lainattaessa yrityksen laitteita matkailija voi helpoiten tarkistaa salausohjelman olemassaolon yrityksensä IT-osastolta. Bitlocker on Microsoftin käyttöjärjestelmien oma kiintolevyn salausohjelma, se tulee valmiina osassa Windows-käyttöjärjestelmissä. Bitlockerin on raportoitu olevan hyvä ja helppo käyttöinen salausohjelma, mutta sillä on kuitenkin omat haittapuolensa. Bitlocker on saatavilla vain tietyille käyttöjärjestelmä versioille, esimerkiksi Windows 7 pi-

tää olla Enterprise- tai Ultimate-versio. Bilockerissa on myös usein epäilty olevan takaovi, koska etenkin lähdekoodi ei ole avoin, mutta takaoven olemassaoloon ei ole todisteita. Bitlockerin luodessa salaukseen avainta se kysyy tietokoneelta numeroa tähän, ja tietokone luo numeron algoritmilla. Snowden paljasti, että NSA on luonut suosittuun algoritmiin, Dual_EC_DRBG, takaoven, jonka avulla salausavaimen arvaaminen nopeutuu huomattavasti. Microsoft kuitenkin väittää, että vaikka kyseinen algoritmi on Windows-käyttöjärjestelmissä, niin sitä ei käytetä Bitlocker-salausavaimen luomiseen [65]. Windowsilla on myös EFS, jonka tarkoituksena on salata tietty kansio tai tiedosto. Erona myös Bitlockeriin EFS tallentaa salausavaimen käyttöjärjestelmälle, kun taas Bitlocker tallentaa laitteen TPM-sirulle. EFS:ssä on riskinä mahdollisuus, että salattu tiedosto vuotaa salaamattomalle alueelle. [65; 66.]

Applen Mac OS X 10.3 ja uudemmissa käyttöjärjestelmissä on FileVault- tai FileVault 2 -salausohjelma valmiina. FileVaultilla ja FileVault 2sella pystyy suojaamaan koko kovalevyn lisäksi ulkoisen muistilaitteen ja erillisiä tiedostoja. Filevault 2sella on ollut isoja haavoittuvuuksia, kuten 2016 hyökkääjä, jolla oli fyysinen pääsy laitteeseen, pystyi saamaan salasanan selkeänä tekstinä [67]. Tämä haavoittuvuus on kuitenkin jo korjattu.

Linuxiin pohjautuvissa käyttöjärjestelmissä on salaamiseen valmiina dm-crypt ja LUKS. Useissa käyttöjärjestelmissä, esimerkiksi Debiassa ja Ubuntussa, salaamisen voi aloittaa jo asennuksen yhteydessä. Kovalevyn voi myös salata asennuksen jälkeen ja on mahdollista salata vain osuuksia. Dm-cryptillä ja LUKS:illa voi salata koko kovalevyn ja yksittäisiä tiedostoja. Näiden käyttö voi kuitenkin olla haastavaa aloittelijalle. [68.]

Matkailijalla on mahdollisuus valmiiden salausohjelmien lisäksi asentaa kolmannen osapuolen salausohjelma. Suosittuja ilmaisia salausohjelmia on etenkin Veracryptin perusversio, GnuPG ja AxCrypt. VeraCrypt perustuu ennen suosittuun TrueCryptiin, jonka turvallisuuden NCC Group julkisesti tutki ja 2015 raportoi, että siinä löydetyt tietoturvariskit eivät kokonaan rikkoneet tiedon luotettavuutta yleisissä käyttötilanteissa [69, s.7]. VeraCryptillä on monia hyviä puolia. Sen pystyy asentamaan moniin eri käyttöjärjestelmiin, Windowsiin, macOS:iin ja Linuxiin. VeraCryptin lähdekoodin tutki 2016 Quarkslab, ja isoimmat ongelmat korjattiin seuraavassa versiossa [70]. VeraCrypt on joustava, se pystyy salaamaan osioita, ulkosen muistilaitteen tai koko kovalevy. Haittapuolena on se, että koko kovalevyn salaaminen toimii vain MBR-partitiontissa, joka on vanhempaa teknologiaa. GnuPG:llä on usealle käyttöjärjestelmälle, esimerkiksi Win-

dowsille, macOS:lle ja Linuxille, suunnattu salausohjelma. GnuPG:llä pystyy salaamaan, yksittäisiä tiedostoja ja viestejä. AxCrypt on Windowsille ja macOS:lle tarkoitettu tiedostojen salausohjelma, joten sillä ei voi salata kovalevyä. AxCrypt tarjoaa monia palveluita, mutta vain maksullisessa versiossaan. Ilmaisessa versiossa käytetään vanhempaa 128-bittistä AES salausta, kun uudessa on 256-bittinen.

5.3 Haittaohjelmien torjuminen

Haittaohjelmien torjunta on tietoturvan perusteita. Haittaohjelmia varten matkustajalla on usein käytössään käyttöjärjestelmässä tulevia omia palomuureja, Windows Defender, mutta on suositeltavaa asentaa myös muita ohjelmia, kuten virustentorjuntaohjelmia Avast Antivirus, Avira Antivir ja Malwarebytes Anti-Malware. Tietoturvan ylläpitämiseen harvoin riittää pelkästään palomuuri, koska mikään ohjelma ei ole 100-prosenttisen turvallinen. Parantaakseen turvallisuutta on siis parempi olla monta tietoturvaohjelmaa samanaikaisesti toimimassa.

Malwarebytes Anti-Malware on usealle käyttöjärjestelmälle suunnattu tietoturvaohjelma haittaohjelmia vastaan. Malwarebytes on tarkoitettu laajempaan haittaohjelmien turvaamiseen, ei pelkästään virusten ja troijalaisten [71]. Haittapuolina ilmaisversiossa on vain Windowsille sopiva, ei reaaliaikaista suojausta ja pitää manuaalisesti aloittaa tietojen tutkimisen haittaohjelmilta. Maksullisessa versiossa nämä haittapuolet korjaantuvat. 2016 Tavis Oramandy löysi Malwarebytesistä haavoittuvuuden, joka mahdollisti mies välissä -hyökkäyksen [72]. Malwarebytes on kuitenkin jo korjannut haavoittuvuuden. Haittapuolina Malwarebytesissä ei ole nopeaa skannausta, eikä sitä ole tarkoitettu aktiiviseksi virustentorjuntaohjelmaksi. [73.]

Avastin Antivirus ja Aviran Antivir ovat molemmat virustentorjuntaohjelmia usealle käyttöjärjestelmälle. Molemmilla on ilmaiset ja maksulliset versiot, jotka tarjoavat eri tason suojaa. Ilmaisversioissa molemmat tarjoavat reaaliaikaista virussuojaa, mutta Aviran on vain Windowsille, kun Avast on Windowsin lisäksi Macille ja Androidille. Kummallakaan ei ole ollut isompia tietoturvahaavoittuvuuksia. Haittapuolena monet suojaukset ovat vain maksullisessa versiossa. [74; 75.]

5.4 Kommunikointi

Matkailijan kommunikoidessa laitteilla tiedon luotettavuus voi helposti rikkoutua. Tätä varten kannattaa suunnitella ja sopia ennen matkalle lähtöä kommunikointi tavat. Osa kommunikointipalveluista ja ohjelmista voi kommunikoida vain saman ohjelman sisällä tai viestin avaamiseen tarvitaan salasana. Valittaessa ohjelmaa ja palvelua matkailijan tulee myös kiinnittää huomiota palvelun tarjoajan sijaintiin, koska valtioilla voi olla eri lait tiedon jakamisesta viranomaisten kanssa. NSA:lla on raportoitu olevan vaikeuksia rikkoa joidenkin kommunikointitapojen salauksia, kuten sähköposti palveluita tarjoavan Zohon ja VoIP:in avainten salaukseen käytettävää ZRTP:ia [43].

Sähköpostia käyttäessä matkailija voi salata viestin toisella ohjelmalla tai käyttää sähköpostipalveluita, jotka salaavat viestin päästä päähän. ProtonMail on sähköpostipalvelu, joka keskittyy tietoturvaan. ProtonMailin palvelimet sijaitsevat Sveitsissä ja ovat näin Yhdysvaltojen ja EU:n lainkäyttövallan ulkopuolella. ProtonMail kertoo Sveitsissä olevien lakien avulla, että ProtonMailiä ei voi pakottaa rakentamaan takaovea järjestelmäänsä ja osallistumaan Yhdysvaltojen tiedusteluvirastojen puolesta tiedon keruuseen [76]. ProtonMail tarjoaa käyttäjiensä keskuudessa oletuksena päästä päähän -salausta ja mahdollisuuden lähettää palvelun ulkopuolisille käyttäjille salasanalla suojattuja viestejä. ProtonMail tarjoaa viestin salaamista salasanalla, jolloin vastaanottajan pitää avata viesti samalla salasanalla. Uhkina ProtonMailissä on myös palveluiden kaatuminen, kuten 2015 DSoS-hyökkäyksen takia pääsy ProtonMailiin oli muutaman päivän ajan mahdotonta [77]. Tulevaisuutta varten ProtonMail on ilmoittanut varautuneensa tuleviin hyökkäyksiin liittoutumalla Radwaren kanssa.

GnuPG on avoimeen lähdekoodiin perustuva salausohjelma, jolla voi salata tiedostot ja viestit. GnuPG on saatavilla usealle käyttöjärjestelmälle: Windowsille, MacOSille, Andoidille ja Linuxille. GnuPG:ssä salaaminen tapahtuu kahdella avaimella: julkisella ja yksityisellä. Julkinen avain on tarkoitettu levitettäväksi julkisesti ja yksityinen avain pidetään salassa. Lähettäessä viestiä tai tiedostoa toiselle tieto salataan vastaanottajan julkisella avaimella. ja salauksen voi avata vain vastaanottajan yksityisellä avaimella [78]. GnuPG:tä tukee muutamat sähköpostipalvelut oletuksena tai liitännäisen kautta, kuten Enigmail-liitännäinen Thunderbird-sähköpostipalveluun.

Signal on salattu kommunikointiohjelma usealle käyttöjärjestelmälle niin puhelimiin kuin tietokoneille, jota myös Snowden käyttää [79]. Signal on ZRTP:hen perustuva avoimen

lähdekoodin ohjelma, ja sen tietoturvallisuus on tutkittu 2017. Tutkimuksessa ei löydetty isoja haavoittuvuuksia, ja Signalin turvallisuusprotokollat täyttää useita standardeja turvallisuustarpeita [80, s.19-20]. Signal on hyvin laaja ohjelma. Se tarjoaa puhelu- ja videopuheita toisiille Signalin käyttäjille [81], tekstiviestejä, tiedostoja [82], kuvia ja videoviestejä verkon kautta. Rajoitteena Signal vaatii käyttäjän puhelinnumeroa tarkistukseen, eikä Signal toimi Windows Phonessa. [83.]

Line ja WhatsApp ovat molemmat hyvin suosittuja pikaviestipalveluita. WhatsApp on Facebookin omistama ja sen päästä päähän -salauksessa käytetään Signalin protokollaa [84]. WhatsApp itse ei ole avointa lähdekoodia, joten sitä ei voi tarkistaa takaovien ja haittaohjelmien varalta. Riskeinä WhatsApp jakaa tietojaan Facebookin kanssa, mikä on mahdollisuus kolmannen osapuolen päästä käsiksi salaamattomiin viesteihin [85]. Line on japanilainen ohjelma, ja sen suurin käyttäjäkunta on japanilaiset. Linessä on myös päästä päähän suojaus, mutta Linelle ei ole tehty mitään tietoturvatutkimuksia. Hyvinä puolina Linessä ja WhatsAppissä on, että ne voi asentaa Windows Phonelle.

5.5 Verkkoselain

Oman verkkoselaimen turvaaminen on nopeaa ja helppoa. Ensimmäisenä matkailijan tulee tarkistaa, että selain on päivitetty. Seuraavana matkailijan voi asentaa tietoturvaa lisääviä liitännäisiä, kuten Ghosteryn, HTTPS-Everywheren ja NoScriptin. Matkailija voi myös käyttää useassa selaimessa valmiiksi olevaa yksityisselausta, joka vähentää selaimen muistiin tallennattavaa tietoa ja estää verkkosivuja seuraamasta käyttäjää.

Liitännäiset usein estävät käyttäjänsä tiedon tallentamisen, kolmannen osapuolen ohjelmien käytön tai pakottavat selaimen käyttämään turvallisempaa yhteyttä. Ghostery on seuraamisen estämiseen liitännäinen. Ghostery tunnistaa sivustolla olevat kolmannen osapuolen seuraimet ja estää näiden toiminnan [86]. HTTPS-Everywhere-liitännäisen tarkoituksena on pakottaa selain käyttämään turvallisempaa HTTPS-yhteyttä, jos sivu tukee HTTPS-yhteyttä [87]. NoScript estää JavaScriptiä toimista ilman käyttäjän lupaa. JavaScriptiä käytetään usealla verkkosivulla ja estämällä JavaScriptin käytön sivut voivat näyttää hyvin erilaisilta. JavaScriptillä on useita tunnettuja haavoittuvuuksia ja jopa 37 % tutkituista sivuista sisälsi ainakin yhden haavoittuvuuksia sisältävän JavaScript-kirjaston [88].

Tor on tuntemattomana pysymiseen tarkoitettu ohjelma. Toria pystyy käyttämään toisen selaimen liitännäisenä, mutta useimmat käyttävät Tor-selainta, joka perustuu Firefoxiin ja sisältää Tor-ohjelmiston lisäksi NoScript- ja HTTPS-Everywhere -liitännäiset. Tor-selain ohjaa käyttäjänsä verkkoliikenteen monien vapaaehtoisten solmuista koostuvan verkoston kautta salatakseen käyttäjän sijainnin. Verkon sisällä Tor salaa verkkoliikenteen, ja viimeisessä solmu purkaa verkoston sisäisen salauksen ja lähettää tiedon alkuperäiseen kohteeseen [89]. Riskinä Tor ei salaa viimeisestä solmusta poistuvaa tietoa, ja tämä viimeinen solmu voi kopioida siitä poistuvaa tietoa. Tätä varten tulisi käyttää päästä päähän suojausta, kuten HTTPS-sivuja. Haittoina Torissa on myös, että Tor hidastaa verkossa käyntiä eikä Tor ole täysin turvallinen. Infosecurity raportoi 2013, että tietyissä tapauksissa Torin käyttäjät voidaan tunnistaa kolmen kuukauden sisällä. [90; 91.]

5.6 VPN

Turvallinen verkkoon liittyminen tapahtuu VPN-palvelun kautta. Luotettavalla VPN-palvelulla matkustaja pystyy käyttämään turvallisemmin julkisia Wi-Fi-yhteyksiä, koska ulkopuoliset eivät pääse tutkimaan liikennettä [92]. VPN-palveluiden tarjoaja kuitenkin tietää käyttäjän IP-osoitteen ja näkee verkkoliikenteen. Suosittuja VPN-palveluita ovat etenkin NordVPN, ExpressVPN, Tunnelbear ja Windscribe. Valittaessa palvelua matkailijan tulee ottaa huomioon, että turvallisimmat versiot VPN-palveluista ovat maksullisia ja ilmaisversioissa voi olla rajoitteita ja mainoksia, esimerkiksi Windscribessä ilmaisversiossa on rajoitettu tiedonsiirto 10 GB per kuukausi [93]. Matkustaja voi käyttää VPN-palvelun sijaan Tor-selainta tehdäkseen itsestään tuntemattoman verkossa, mutta Tor ei salaa liikennettä Tor-verkoston ulkopuolella. [94.]

NordVPN ja ExpressVPN ovat molemmat luotettuja palveluita. Haittapuolena näissä on, ettei niissä ole ilmaisversioita. Molemmat ovat Linuxille, Windowsille, macOS:lle, iOS:lle ja Androidille suunnattuja, mutta ExpressVPN:än voi myös asentaa BlackBerrylle. Molemmat ovat Yhdysvaltojen ulkopuolella toimivia, sallivat vertaisverkon, tarjoavat 256-bittistä AES -salausta ja OpenVPN-protokollaa, joka määrää, miten VPN luo turvallisen päästä päähän -yhteyden [95]. Marc Bevand raportoi 2016, että ExpressVPN käyttävän 1024 bittistä RSA -avainta OpenVPN:ssä, mutta ExpressVPN tiedotti korjanneensa ja siirtyneensä 2048 bittisiin avaimiin [96].

Tunnelbear ja Windscribe tarjoavat rajoitettuja ilmaisversioita. Molemmat ovat Linuxille, Windowsille, macOS:lle, iOS:lle ja Androidille. Molemmat tarjoavat 256-bittistä AES-salausta Windscribe rajoittaa tiedonsiirron 10 GB per kuukausi ja Tunnelbear tarjoaa 500 MB per kuukausi. Cure53 teki 2016 ja 2017 Tunnelbearille tietoturvatutkimukset. 2017 Cure53 raportoi Tunnelbearin korjanneen isot tietoturvahaavoittuvuudet. Kriittisiä haavoittuvuuksia ei havaittu, mutta muutamia haavoittuvuuksia löydettiin [97]. TunnelBear myös estää vertaisverkot [98]. Windscribestä ei ole saatavilla tietoturvatutkimuksia, mutta se tarjoaa vertaisverkkoa ja erikoisuutena omaa palomuuria Windowsille ja macOSlle. [99]

5.7 Tallentaminen

Matkan aikana matkailijan kannattaa miettiä, mihin tallentaa tietonsa: laitteen omalle muistille, ulkoiselle muistilaitteelle vai pilvipalveluun. Varkauden tapahtuessa laitteisiin tallennetut tiedot katoavat ja ovat riskinä paljastua, joten pilvipalvelun käyttämisen harkitseminen on tärkeää. Koska tieto voi kuitenkin vuotaa pilvipalvelulle siirrettäessä tai varastoituessa, niin tiedon salaaminen ennen tapahtumaa on tärkeää, esimerkiksi AxCryptin avulla. Snowden suosittelee Dropboxin lopettamista ja siirtymään esimerkiksi SpiderOakiin [100].

SpiderOak on pilvipalvelu usealle käyttöjärjestelmälle. SpiderOak tarjoaa päästä päähän -salausta ja käyttää No Knowledge -käytäntöä. Käytännössä SpiderOakilla ei ole tietoa käyttäjiensä tietojen sisällöstä tai nimistä [101]. Haittapuolena SpiderOak sijaitsee Yhdysvalloissa, on maksullinen ja sen lähdekoodi ei ole kokonaan avointa.

5.8 Usb-muistilaitteen käyttäminen käyttöjärjestelmänä

Käyttämällä ulkoisissa muistilaitteissa, kuten USB-muistitikuissa, olevia käyttöjärjestelmiä matkustaja pystyy kantamaan tietojaan helposti mukanaan ja käyttää omaa käyttöjärjestelmäänsä muissa laitteissa. Ulkoisissa muistilaitteissa useimmiten on kuitenkin vähemmän muistitilaa. Tällöin hän pystyy käyttämään vain perusohjelmia, ja tiedon siirto on hitaampaa. Päästääkseen vielä tietoihin matkustaja tarvitsee silti laitteen. Snowdenin suosittelema Tails-käyttöjärjestelmä on USB-muistitikulle suunnattu ja tarkoitettu käytettäväksi jopa luottamattomissa laitteissa [102]. Snowdenin suosittelema Qubes

OS:n pystyy asentamaan USB-muistitikulle, mutta tämä on vielä alpha-vaiheessa. [103.]

Tails on Debianiin pohjautuva käyttöjärjestelmä, joka keskittyy turvallisuuteen tuntematomana pysymisen ja yksityisyyden kautta. Tailsin mukana tulevat tarvittavat ohjelmat. Tailsin on rakennettu olemaan käyttämättä tietokoneen kovalevyä ja muistin varastoimisen kannalta vain RAM:ia, jolloin tietokoneen sammuessa Tailsin käytöstä ei jää jälkiä. Tails ei kuitenkaan suojaa hardwaressa olevilta haittaohjelmilta, BIOS:in ja firmwaren kautta tulevilta hyökkäyksiltä, eikä Tails salaa tiedostoja ja poista metadataa oletuksena [104]. Tails ei myöskään piilota käyttäjänsä käyttävän Toria ja mahdollisesti olevan Tailsin käyttäjä, eikä Tails toimi kaikilla laitteilla. 2014 NSA:n on raportoitu keräävän tietoa käyttäjistä, jotka käyvät Tailsin verkkosivuilla tai edes tekevät verkkohakuja Tailsiin liittyen [105].

5.9 Salasanat

Monien vahvojen salasanojen muistaminen voi olla haastavaa, joten näiden tallentaminen muistiin on mahdollisuus. Verkkoselaimet tarjoavat salasanojen tallentamista, mutta laitteen varkaudeksi joutumisessa varas myös pääsee helposti sisään tunnuksille. Toinen vaihtoehto on salasanamanagerit. Salasanamanagerit varastoivat ja salaavat tallennetut salasanat yhden pääsalasanan avulla. Ne voivat olla paikallisesti asennettava ohjelma tai pilvessä sijaitseva palvelu. Kummallakin on omat hyvät ja huonot puolensa, kuten paikallinen ohjelma ei vaadi verkkoa toimiakseen, mutta laitteen katoamisessa katoavat myös salasanat. Pilvipalveluissa matkailija ei ole rajoittunut tiettyyn laitteeseen, mutta tieto voi vuotaa tiedonsiirron aikana ja käyttäjä tarvitsee verkkoyhteyden päästäkseen käsiksi salasanoihinsa. Osa salasanamanagereista on paikallisen asennuksen ja pilvipalvelun yhdistelmiä, joissa tieto tallennetaan pilvipalvelulle, mutta tietoja käsitellään paikallisesti asennetulla ohjelmalla.

Suosittuja salasanamanagereita on Dashlane, KeePass, Keeper ja Encryptr. Dashlane on Mac OSlle, Windowsille, iOSlle ja Androidille suunnattu paikallisesti asennetta salasanamanageri, jossa on pilvipalvelusynkronointi. MIT tutki 2016 Dashlanen turvallisuuden ja raportoivat, etteivät löytäneet isoja haavoittuvuuksia, ja he totesivat:

> Kaiken kaikkiaan löysimme Dashlanen olevan aika turvallinen kaikkia hyökkäyksiämme vastaan. [106, s. 12.]

KeePass on ilmainen avoimen lähdekoodin salasanamanageri, joka on suunnattu Windowsille. KeePassistä on tehty tietoturvatutkimus, joka raportoi KeePassin olevan tietoturvallisesti hyvä [107]. KeePassistä on olemassa epävirallisia versioita Androidille, iOSlle, Mac OSlle ja Linuxille. KeePassiin perustuvia salasanamanagereita on myös olemassa, kuten Linuxille pääasiassa suunnatut KeePassX ja KeePassXC, mutta näiden turvallisuutta ei ole tutkittu. Keeperin salasanamanageri on usealle käyttöjärjestelmälle suunnattu ja tulee tehdasasetuksena Windows 10-käyttöjärjestelmille. Keeperillä on raportoitu olevan isoja haavoittuvuuksia, kuten Googlen tietoturvatutkijan Tavis Ormandyn 2017 joulukuussa löytämä haavoittuvuus, jossa Keeperin verkkoselainliitännäinen vuosi verkkosivuille salasanoja. Keeper kuitenkin korjasi haavoittuvuuden 24 tunnin sisällä [108]. Encryptr on avoimen lähdekoodin pilvipalvelusalasanamanageri, joka on suunnattu usealle käyttöjärjestelmälle. Encryptrin tietoturvallisuutta ei ole tutkittu, mutta sen omistama SpiderOak on Snowdenin suosittelema.

6 Vaiheittainen ohje matkailijalle oman tietoturvan rakentamisessa laitteisiin

Tässä osiossa rakennan vaiheittaisen ohjeen oman tietoturvan parantamiseksi jo käytössä oleville laitteille, miten asentaa turvallinen Ubuntu ja miten asentaa tietoturvallisuuteen perustuva käyttöjärjestelmä, Tails, USB-muistitikulle. Käyttämieni laitteiden tiedot:

- Asus G55VW-S1177H, Windows 8.1
- HTC One M8, Android-versio 6.0, HTC Sense -versio 7.0
- Kingston DataTraveler 100 G3 16 GB.

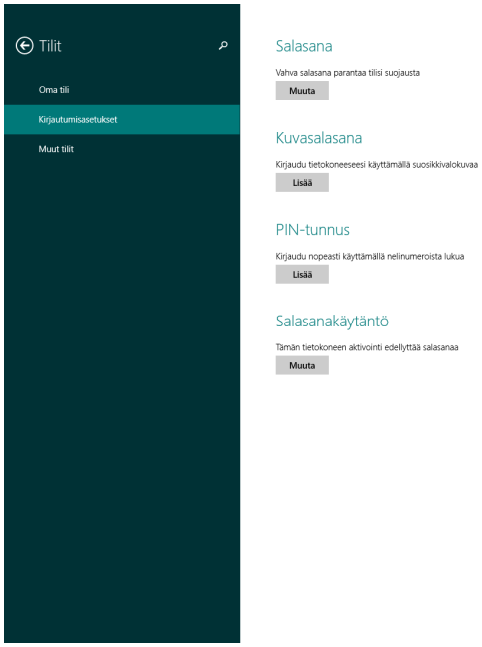
6.1 Windowsin turvaaminen

Ohjeessa annan BIOS:ille ja käyttäjätunnukselle salasanat, kiellän ulkoisilta muistilaitteilta käynnistämisen, suojaan selaimeni, asennan haittaohjelmia vastaan kaksi torjuntaohjelmaa, asennan VPN-palveluna WindScriben, salasanamanagerina Dashlanen ja

pilvipalvelua varten SpiderOak ONE:n. Lopuksi salaan kovalevyn VeraCrypt-salausohjelmalla.

Windowsin valmistelu alkaa BIOS:in salaamisella ja mahdollisesti ulkoisilta muistilaitteilta käynnistämisen kieltämisellä, jos näitä ei itse tarvitse. Kannattaa huomioda, että BIOS-valinnat riippuvat laitteesta ja voivat olla erilaiset, kuin ohjeessa. BIOS:iin pääsee laitteen käynnistyksen aikana painamalla näppäintä. Näppäin riippuu laitteesta, ja Asuksella tämä on Delete. Käynnistetään laite ja aletaan painella näppäintä samantien, noin kaksi kertaa sekunnissa. Siirrytään ”Security”-välilehdelle ja valitaan ”Administrator Password”. Annetaan salasana, vahvistetaan ja BIOS ilmoittaa ”Password Installed”. Seuraavaksi tarkistetaan, että ”Secure Boot Control” on päällä. Mennään kohtaan ”Save & Exit” ja valitaan ”Save Changes and Exit” sekä ”Yes”.

Seuraavana asennetaan käyttäjälle salasana. Käynnistetään ”Ohjauspaneeli”, valitaan ”Käyttäjätilit”, ”Tee muutoksia tiliin tietokoneen asetuksissa” ja ”Kirjautumisasetukset”. Nähdään kuvan 3 mukaisen näkymän. Valitaan ”Salasanakäytäntö” kohdasta ”Muuta” ja annetaan salasana tilille ”Salasana” kohdan alla olevasta ”Muuta”.



Kuva 3. Näkymä salasana vaihtoehdoista.

Seuraavaksi voidaan suojata selain tai käyttää selaimessa olevaa yksityisyys-välilehteä, jota käyttämällä selain ei tallenna selaushistoriaa, evästeitä, tilapäistiedostoja ja hakuja. Selaimen, Firefoxin, suojaaminen tapahtuu avaamalla selain ja kirjoittamalla URL-tekstikenttään ”about:preferences#privacy”. Näkyville tulee turvallisuus ja

yksityisasetukset. Poistetaan päältä ”Remember logins and passwords for websites”, ”Allow Firefox to send technical and interaction data to Mozilla”. Laitetaan päälle ”Tracking protection” valitsemalla ”Always”. Seuraavaksi asennetaan liitännäiset tietoturvan lisäämäksi. Kirjoitetaan URL-tekstikenttään ”about:addons”, valitaan ”Get Add-ons” ja painetaan ”See more add-ons!”. Hakukentän avulla etsitään ja valitaan ”Ghostery”, paina ”+ Add to Firefox” , ”Add” ja otetaan pois päältä ”Share my analytics and Human Web data to improve Ghostery’s performance.”. Seuraavaksi etsitään ”Noscript”, ”+ Add to Firefox” ja ”Add”. Viimeisenä etsitään ”HTTPS Everywhere” ja valitaan ”+ Add to Firefox” ja ”Add”.

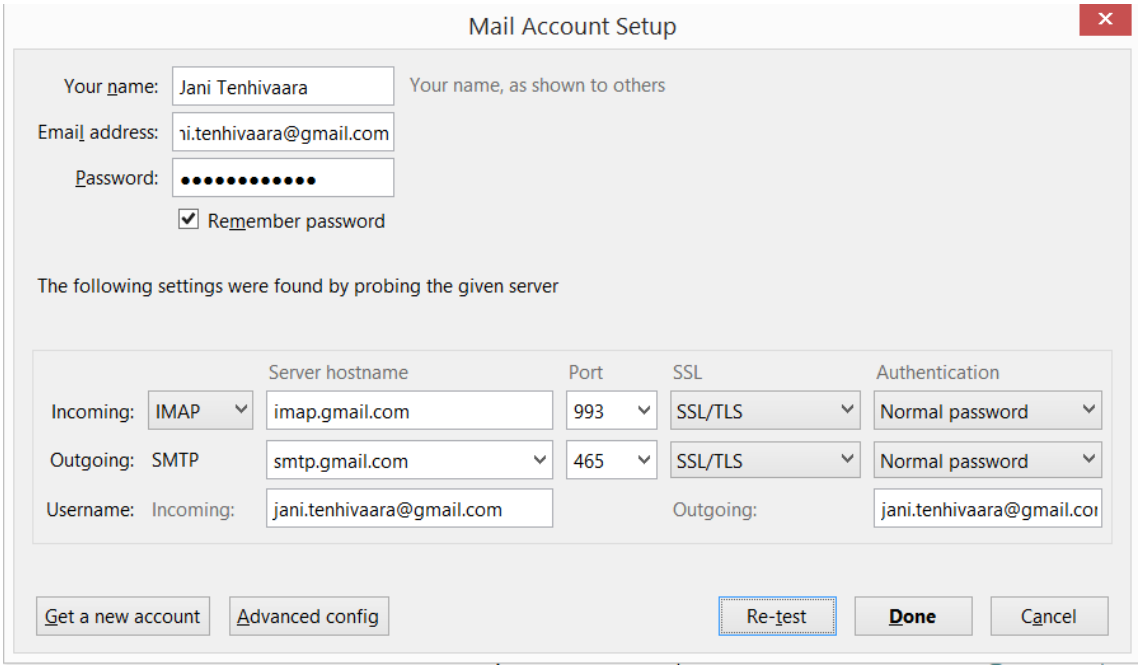
Virustentorjuntaohjelmina asenetaan samanaikaisesti Malwarebytes ja Antivir. Aloitetaan Antivirin asennuksella, jonka voi ladata sivulta "https://www.avira.com/en/free-security-suite". Avataan ladattu tiedosto ja aloitetaan painamalla "Accept and install". Jos tietokone kysyy lupaa sallia tiedoston tekevän muutoksia, valitaan "Yes". Muutaman minuutin jälkeen Antivir on asentunut. Antivir-virustentorjuntaohjelman mukana tukee myös Phantom VPN-palvelu, jonka kautta voidaan käyttää VPN-palvelua 500 MB ajan, ja Password Manager, johon voit tallentaa salasanasi. Käyttääkseen Phatom VPN:ää, avataan Avira ja valitaan "Connect". Käyttääkseen Password Manageria, avataan selaimen liitännäisset, painetaan "enable" ja mennään sivulle "https://passwords.avira.com/login". Täältä voi kirjautua sisään palveluun.

Malwarebytesin asentaminen alkaa lataamalla ohjelma sivulta "https://www.malwarebytes.com/pricing/". Avataan ladattu tiedosto, sallitaan tiedoston tekevän muutoksia, valitaan kieli ja painetaan "Accept and install". Hetken kuluttua ohjelma on asennettu. Jos asensit ilmaisversion, niin huomioi, että ilmaisversiossa tiedostot pitää manuaalisesti skannata haittaohjelmien varalta. Tämä voidaan tehdä avaamalla Malwarebytesin ja painamalla "Scan now".

Sähköpostina käyttäjä voi valita suoraan ProtonMailin tai hankkia GnuPG-salaaminen. Ohjeet ovat molempiin. ProtonMailin voi helposti hankkia menemällä sivulle ”https://protonmail.com/”, valitsemalla ”Get your encrypted email account” ja valitsemalla ,minkä vaihtoehdoista haluaa. Seuraavaksi täytetään käyttäjätiedot ja todistetaan olevan ihminen painamalla ”I’m not a robot”. Suojaamalla paremmin tilin, laitetaan päälle kaksivaiheinen tunnistautuminen. Tätä varten tulee olla jokin ohjelma tunnistautumista varten toisella laitteella. Käytän ohjeessani ”Google Authenticator” ohjelmaa, jonka olen ladannut Play-kaupan kautta puhelimelleni. Kaksivaiheinen tunnistautuminen laite-

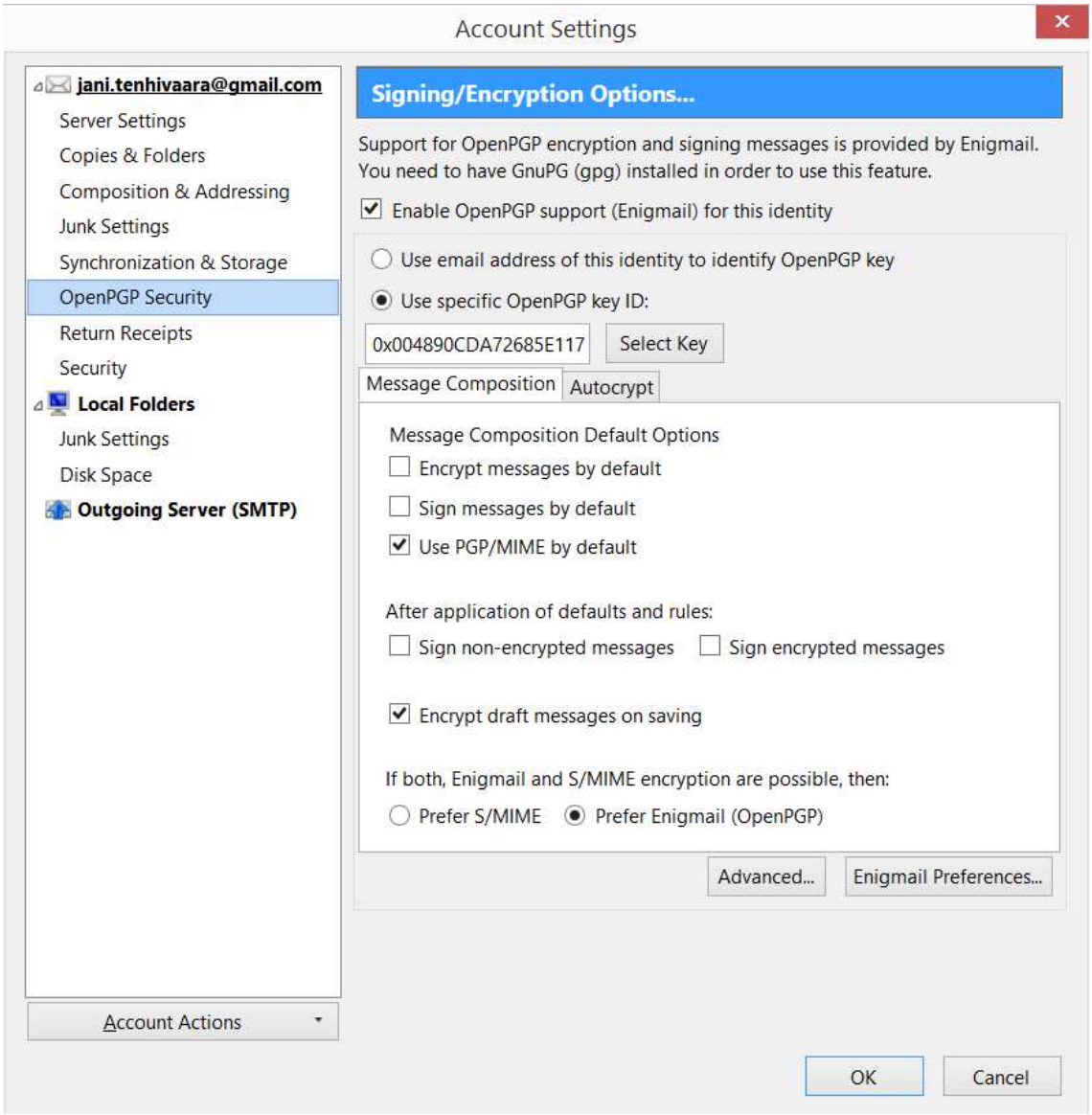
taan päälle avaamalla ”SETTINGS”, ”Security” ja valitsemalla ”ENABLE TWO-FACTOR AUTHENTICATION”. Avaan samalla puhelimestani ”Google Authenticator” ja valitsen ”Anna saamasi avain”. ProtonMailistä valitsen ”Next” ja ”Enter key manually”. Lisään puhelimeeni tilin nimen ja ProtonMailistä saamani koodin. Seuraavaksi annan ProtonMailille salasanani ja puhelimessani olevan koodin. Paina ”Next”. Otetaan talteen koodit ProtonMailistä, jos katoaa tunnistautumismenetelmä, niin voidaan koodeilla kirjautua sisään. Jatketaan painamalla ”OK” ja valmis.

ProtonMailin vaihtoehtona voidaan käyttää OpenPGP-salausta GnuPG:n kautta. Ohjeessa käytän Thunderbirdin kautta Gmail-sähköpostiliäni ja Enigmail-liitännäistä GnuPG:n lisäksi. Aloitetaan lataamalla GnuPG sivulta "https://gnupg.org/download/index.html#sec-1-2". Valitaan "download"-kohdan "Simple installer for the current GnuPG" vierestä. Ladataan seuraavaksi Thunderbird-sivulta "https://www.thunderbird.net/en-US/". Avataan ladattu GnuPG ja sallitaan sen tehdä muutoksia. Valitaan seuraavaksi kieli ja painetaan "OK". Asennetaan ohjelma painamalla "Next", "Next", "Install", "Next" ja "Finish". Seuraavaksi asennetaan Thunderbird avaamalla ladattu Thunderbird-tiedosto ja sallitaan sen tehdä muutoksia painamalla "Yes". Asennetaan ohjelma painamalla "Next", "Next", "Install" ja "Finish". Thunderbird avautuu ja kysyy asetuksia. Valitaan "Set as Default". Koska käytän olemassa olevaa Gmail-tunnusta, niin valitsen "Skip this and use my existing email". Jos käytössä on Gmail, niin painetaan "Advanced config". Kuvan 4 mukaan syötetään omat käyttäjäsi tiedot ja syötetään asetuksiin "Incoming"-kohdalle palvelimen nimeksi "imap.gmail.com", portiksi 993, valitaan "SSl/TLS" ja "Normal password". "Outgoing"-kohdalle serverin nimeksi "smtp.gmail.com", portiksi "465", valitaan "SSL/TLS" ja "Normal password". Lopuksi syötetään "username"-kohtaan sähköpostitilin osoitteen. Syötetään salasanakohtaan Googlen ohjelmakohtaista salasana, jonka saa sivulta "https://support.google.com/mail/answer/185833?hl=en&rd=1", kunhan Googlen kaksivaiheinen tunnistautuminen on päällä. Lopuksi painetaan "Re-Test" ja "Done".



Kuva 4. Gmail-asetusten tiedot.

Lisätään Thunderbirdin turvallisuutta, otetaan HTML pois päältä. Painetaan menu-näppäintä, valitaan "View", "Message Body as" ja "Plain text". Seuraavaksi poistetaan evästeet, avaamalla menu, valitsemalla "Options" ja "Options". Avataan "Privacy"-välilehti ja otetaan pois päältä valinnat "Remember websites and links I've visited" ja "Accept cookies from sites". Seuraavaksi ladataan ja asennetaan Enigmail. Avataan Thunderbird ja painetaan menu-näppäintä ja valitaan "Add-ons". Menemällä "Extensions"-välilehdelle, etsitään Enigmail ja painetaan "Install". Seuraavaksi luodaan uusi salasana salausavaimella ja luodaan kumoussertifikaatti. Painetaan menu-näppäintä, valitaan "Enigmail" ja "Key management". Painetaan "Generate" ja "New Certificate". Valitaan minne tallennetaan ja painetaan "save". Salasanan luodaan painamalla "File" ja "Change passphare". Syötetään salasana kahdesti ja painetaan "OK". Seuraavaksi muokataan Thunderbird toimimaan Enigmailin kanssa. Painetaan menu-näppäintä ja valitaan "Options" ja "Account Settings". Valitaan "OpenPGP Security" ja "Use PGP/MIME by default", kuvan 5 mukaisesti.



Kuva 5. OpenPGP asetukset.

Jotta salaaminen onnistuu, niin käyttäjällä ja vastaanottajalla pitää olla toisten julkiset salausavaimet. Tämän vaihtaminen onnistuu kirjoittamalla toisen sähköpostin ja liittämällä siihen julkisen avaimen. Painetaan "Write", "Enigmail" ja "Attach My Public Key". Kirjoitetaan viesti normaalisti ja painetaan "Send". Kun saa toiselta viestin, jossa on vastaanottajan julkinen avain, painetaan "Import Key","Yes" ja "OK". Jos kuitenkin ladataan julkinen avaimen verkosta, niin avataan menu, painetaan "Enigmail" ja "Key Management". Täältä painetaan "File ja Import Keys from File". Valitaan ladattu avaintiedosto ja painetaan "Open", "Yes" ja "OK". Lähettääkseen salattuja viestejä, niin tulee olla vastaanottajan julkinen avain. Kun on saatu julkinen avain, painetaan "Write" ja kirjoitetaan viesti. Enigmail tunnistaa automaattisesti tämän ja salaa viestin. Kun saa salatun viestin, avataan se ja syötetään salausavaimen salasana ja painetaan "OK". Vahvistaakseen jonkun toisen julkisen avaimen, pitää olla luotetusti yhteydessä häneen,

esimerkiksi fyysisesti tapaamalla, ja tarkistaa julkisen avaimen sormenjälki. Sormenjälki on uniikki koodi jokaiselle avaimelle ja se näkyy, kun avataan Thunderbirdin, avataan menu, valitaan "Enigmail" ja "Key Management". Kaksoisklikataan avainta ja nähdään "Fingerprint"-kohdassa avaimen sormenjälki.

Pilvipalveluun käytän SpiderOak ONE:a. Ladataan tämä sivulta "https://spideroak.com/one/". Avataan tiedosto, valitaan "Next", "I accept the terms in the License Agreement" ja "Next". Seuraavaksi voidaan valita, minne ohjelma asennetaan valitsemalla "Browse" tai annetaan ohjelman asentua oletuspaikkaansa. Valitaan "Next" ja "Install". Sallitaan ohjelman tehdä muutoksia. Jos asennus haluaa sulkea jotain muita käynnissä olevia ohjelmia jatkaakseen, valitaan "OK". Lopuksi valitaan "Finish". Tiedostoja voidaan ladata pilvipalveluun valitsemalla tiedosto hiiren oikealla painikkeella ja valinnan "SpiderOakONE" alta valitaan "Add to Backup". Nähdäkseen pilvipalvelussa olevat tiedostot, avataan SpiderOakONE-ohjelma, ja "Manage"-välilehden alla on kaikki tallennetut tiedostot.

Dashlane-salasanamanagerin asentaminen alkaa lataamalla ohjelma sivulta "https://www.dashlane.com/download". Avataan tiedosto, sallitaan tiedoston tehdä muutoksia ja valitaan "Create your free account". Annetaan käyttäjätietot ja valitaan "Next". Vahvistetaan salasanasi ja valitaan "I know it. Let's go". Valitaan "Next", "Next", "Next" ja "Review your passwords". Dashlane oletuksena tuo ja tallentaa selaimen muistissa olevat salasanat. Jatketaan painamalla "Import", "OK" ja "Add Dashlane to Firefox". Selain aukeaa ja valitaan "Add it now. Finish set up!", "Allow", "Add" ja"OK". Seuraavaksi voi laitaa kaksivaihetunnistautumisen päälle avaamalla Dashlane-ohjelma ja paina ctrl+O, jolloin asetukset aukeavat. Valitaan "Security"-välilehti ja avataan asetukset muutettavaksi painamalla vasemmalla alhaalla olevaa lukkoa ja antamalla salasana. Mennään "Two-Factor Authentication"-välilehdelle ja laitetaan tämä päälle. Jkaksivaihetunnistautuminen toimisi, tarvitaan verkkoyhteys. Turvallisuuden lisäämiseksi valitaan "Each time I log to Dashlane" ja "Next". Nähdään mitä tunnistautumis menetelmiä voidaan käyttää ja valitaan "Next". Yhdistetään Dashlane tunnistautumissovellukseen, valitaan "Next" ja syötetään varapuhelinnumero. Lopuksi voi tallentaa Dashlanen antamat koodit, jos kadottaa tunnistautumismenetelmän ja painetaan "Done" ja "OK".

WindScribe VPN-palvelun käyttöönottaminen alkaa lataamalla ohjelma sivulta "https://windscribe.com/download". Avataan tiedosto ja sallitaan sen tehdä muutoksia.

Valitaan kieli ja painetaan "Next". Luodaan seuraavaksi käyttäjätunnus. Käyttääkseen WindScribea avataan se ja painetaan ON/OFF-näppäintä, jolloin VPN-palvelin kytkeytyy päälle. Tarvittaessa voidaan myös vaihtaa palvelinta samalta sivulta.

Lopuksi salaan kovalevyn VeraCrypt-salausohjelmalla. Asennetaan VeraCrypt-sivulta ”https://www.veracrypt.fr/en/Downloads.html”. Palautus ISO-imagea varten laitetaan tietokoneeseen tyhjä ja tallentava CD- tai DVD-levy. Avataan Veracrypt ja valitaan ”Create Volume”. Koska salataan kovalevy, jolla Windows sijaitsee niin valitaan ”Encrypt the system partition or entire system drive”, ”Next”, ”Next”, ”Encrypt the whole drive” ja ”Next”. Seuraavassa osiossa, jos ei käytä RAID:ia, valitaan ”Yes” ja ”Next”. Tietokone mahdollisesti kysyy lupaa jatkaa, johon vastataan ”Yes”. Valitaan ”Single-boot”, ”AES(Twofish(Serpent))”, ”Next”, ”Yes” ja ”OK”. Seuraavaksi annetaan salasana ja vahvistetaan tämä. Salasanan tulee olla monimutkainen ja pitkä, jotta tietoturva säilyy. Painetaan ”Next” ja seuraavaksi voidaan heilutella hiirtä wizard-ikkunan sisällä, joka satunnaistaa salauksen. Lopuksi painetaan ”Next”, ”Yes”, ”Next”. Seuraavaksi luodaan palautus ISO-image, jos jotain menee pieleen. Valitaan ”Browse”-näppäimellä minne tallennetaan palautus ja painetaan ”Next”, ”OK” ja ”Burn”. Valitaan ”Next” ja ”OK”. VeraCrypt tarkistaa, että palauslevy toimii. Jatketaan painamalla ”Next”, valitaan Wipe moodiksi ”3-pass (US DoD 5220.22-m)” tai jokin muu haluttu, koska 3-pass valinnalla salaaminen kestää neljä kertaa kauemmin kuin 1-pass, ja painetaan ”Next”. Jos on valittu joku wipe moodi, niin painetaan ”Yes”. Painetaan ”Test”, jolloin VeraCrypt tarkistaa kaiken toimivan oikein. Valitaan ”Ok” ja ”Yes”, jolloin tietokone käynnistyy uudestaan. Tietokoneen käynnistyksen jälkeen VeraCrypt pyytää aikaisempaa salasanaa, joten annetaan se. PIM-koodia ei ole luotu, joten sen voi jättää tyhjäksi ja painetaan enteriä. Kirjaudutaan sisään ja VeraCrypt ilmoittaa testin olevan valmis. Aloitetaan salaaminen painamalla ”Encrypt” ja ”OK”. Tietokone voi kysyä lupaa, jolloin painetaan ”Yes”. Riippuen valinnoista salaaminen voi kestää tunteja. Kun salaaminen on valmis, painetaan ”OK” ja ”Finnish”. Kovalevy on salattu. Kun käynnistää tietokoneen, joutuu antamaan VeraCryptin salasanan ja tietokone käynnistyy tämän jälkeen normaalisti.

6.2 Androidin turvaaminen

Käytän puhelimeni suojaamiseen puhelimessa tulevia ohjelmia, Windscribe VPN-palvelua, Signalia kommunikointiin, SpiderOak Onea pilvipalveluna, Encryptriä salasana managerina ja AxCryptiä avaamaan pilvipalvelussa olevani tiedostot.

Aloitetaan puhelimen turvaaminen salasanoilla. Mennään ”Asetukset”, ”Suojaus”, ”Aseta SIM-kortin lukitus”. Täältä tarkistetaan, että ”Lukitse SIM-kortti” on päällä ja vaihdetaan SIM-kortin PIN-koodi paremmaksi valitsemalla ”Vaihda SIM-kortin PIN”. Näppäillään vanha PIN-koodi ja valitaan uudeksi 8 numeroisen PIN-koodin. Syötetään uusi PIN-koodi uudestaan ja puhelin ilmoittaa näytön alareunassa vaihdon onnistuneen. Seuraavaksi laitetaan näppäinlukko päälle menemällä kerran taaksepäin ”Suojaus”-asetuksiin. Ylhäältä valitaan ”Ruudun lukitus”. Koska minulla oli vanha PIN-koodi, niin syötän tämän. Seuraavaksi valitaan ”PIN-koodi”-valinta ja otetaan ”Yksinkertainen PIN” valinta päälle. Seuraavaksi valitaan pitkä PIN-koodi, joka on eri kuin SIM-kortin PIN-koodi. Painetaan ”Jatka” ja näppäillään sama numero uudestaan. Salasanojen jälkeen ”Suojaus”-asetuksista laitetaan vielä päälle ”Virtapainike: välitön lukitus” ja ”Saapuvat puhelut” ja varmistetaan, että ”Tuntemattomat lähteet” on pois päältä, jolloin tuntemattomista lähteistä ei asenneta sovelluksia.

Seuraavaksi varmistetaan, että varkauden tapahtuessa pystyt etähallitapuhelinta. Mennään ”Asetukset”, ”Sijainti” ja varmistetaan, että sijainti on ”ON”-tilassa, jolloin etähallinalla voi etsiä laitteen. Seuraavaksi mennään taaksepäin takaisin ”Asetukset”-välilehdelle ja valitaan ”Google”, ”Tietoturva”, ”Paikanna puhelin”. Täältä varmistetaan, että etähallinta on ”Käytössä”. Käydään myös samalla tarkistamassa, että ”Google Play Protect” on päällä. Mennään taaksepäin takaisin ”Tietoturva”-välilehdelle ja valitaan ”Google Play Protect”. Sivun alhaalta tarkistetaan, että ”Tarkista laitteen turvallisuusuhat” on päällä.

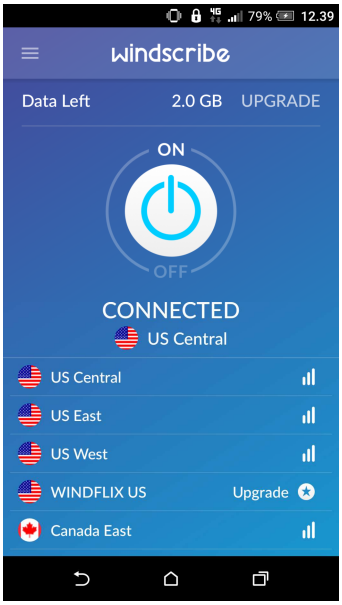
Seuraavaksi tarkistetaan päivitykset ja laitetaan turhat verkot pois päältä. Mennään ”Asetukset”, ”Tietoja”, ”Ohjelmistopäivitykset”. Alhaalla on kohta ”Tarkista Nyt” ja painamalla sitä tulee ilmoitus onko päivityksiä. Valitaan "OK". Seuraavaksi siirrytään takaisin ”Asetukset”-välilehdelle ja laitetaan pois päältä ”Wi-Fi” ja ”Bluetooth”. Seuraavaksi valitaan ”Lisää” ja laitetaan ”NFC” pois päältä. Tarkistetaan vielä, ettei puhelimen Wi-Fi hotspot ole päällä, valitsemalla ”Matkapuhelinverkon jakaminen” ja katsotann, että ”Wi-Fi Hotspot” on pois päältä.

Selaimena käytän oletuksena tulee Chromea. Sen tietoturvaa parannetaan avaamalla Chrome ja valitaan ”Asetukset”, ”Salasanojen tallentaminen”. Ota pois päältä ”Salasanojen tallentaminen” ja ”Automaattinen kirjautuminen”. Seuraavaksi mennään taaksepäin takaisin ”Asetukset”-välilehdelle ja valitaan ”Tietosuoja”. Varmista, että tehdasoletuksena selaussuoja on päällä. Seuraavaksi valitaan ”Do Not Track” ja laitetaan tämä

päälle. Tämän jälkeen varmistetaan, että sivustot eivät tallenna evästeitä menemällä taaksepäin takaisin ”Asetukset”-välilehdelle ja valitaan ”Sivustoasetukset”. Täältä valitaan ”Evästeet” ja otetaan ”Evästeet” pois päältä. Varmuuden vuoksi matkalla voi käyttää vielä incognito-välilehteä verkossa selailuun, jonka tässä versiossa voi avata käynnistämällä Chrome-selain, painamalla oikealta kolmipallovalintaa ja valitsemalla ”Uusi incognito-välilehti”.

Kommunikointiin käytän Signalia. Avataan Google Play -kauppa, josta etsitään Signal ja asennetaan tämä. Asentamisen jälkeen avataan sovellus ja annetaan sovellukselle lupa yhteystietoihin ja mediaan painamalla ”jatka” ja seuraaviin lupiin myös painamalla ”Salli”, ”Salli”, ”Salli”. Seuraavaksi kirjoitetaan oma puhelinnumero ja painetaan ”Rekisteröidy”, ”Jatka”, ”Salli”. Signal lähettää vahvistustekstiviestin ja Signal otti siitä automaattisesti vahvistuskoodin. Seuraavaksi annetaan profiilille nimi ja painetaan ”Valmis”. Koska Signalin salaus toimii käyttäjien kesken, niin varmistetaan, että kohdehenkilö myös käyttää Signalia. Seuraavaksi lisätään kohdehenkilön numero ja varmistetaan Signalin toimivan lähettämällä tekstiviesti. Painetaan oikealta ylhäältä olevaa suurennoslasia, etsitään kohdehenkilö nimellä tai puhelinnumerolla, valitaan kohdehenkilö ja painetaan enter. Lopuksi varmistetaan, että kohdehenkilö on oikea ja hänen salausavain on oikea. Tämä tapahtuu, kun fyysisesti tavataan kohdehenkilö. Tällöin ensin avataan Signal ja viestintänäyttö. Seuraavaksi avataan asetukset painamalla oikealta ylhäältä kolmipallopainiketta ja valitaan ”Conversation settings”. Täältä valitaan ”Verify safety numbers” ja nähdään QR-koodi ja numerosarjoja. Tämä on uniikkikoodi jokaiselle eri kontaktille. Kohdehenkilö tekee saman ja ottaa myös QR-koodin esille. Voidaan verrata numeroita, ja jos ne ovat samat, niin salaus toimii. Toisena vaihtoehtona toinen voi painaa omaa QR-koodiansa, jolloin kamera tulee päälle, ja kohdistaa kameran toisen henkilön QR-koodiin. Jos salaus toimii, niin QR-koodi muuttuu vihreäksi palloksi. Jos salaus ei ole oikea, niin QR-koodi muuttuu punaiseksi palloksi.

VPN-palveluna käytän WindScribeä, jonka asennan Google Play -kaupasta. Kun WindScribe on asentunut, niin avataan tämä. Luodaan uusi käyttäjä tai kirjaudutaan vanhalla. Kun on kirjautunut sisään, painetaan keskellä olevaa ON/OFF-näppäintä, jolloin kytkeydytään sisään (kuva 6). Tarvittaessa voidaan alempaa valita haluttu palvelimen.



Kuva 6. VPN-palvelu WindScriben päälle laittaminen.

Salasanamanagerina käytän Encryptr-ohjelmaa, jonka voi asentaa Google Play -kaupasta. Asentamisen jälkeen avaa ohjelma ja jos tämä on ensimmäinen käyttökerta, valitse ”New to Encryptr?”. Valitse käyttäjätunnus ja salasana ja valitse ”Sign up”. Uuden salasanan voi luoda painamalla punaista plussaa ja valitsemalla ”PASSWORD”. Seuraavaksi syötä tarvittavat tiedot salasanaa kohden ja valitse oikealta ylhäältä oikeinmerkki jatkaaksesi. Nyt olet tallentanut salasanasi.

Pilvipalveluna käytän SpiderOak ONE:a, jonka voi myös ladata ja asentaa Google Play -kaupan kautta. Kun ohjelma on asentunut, avataan se. Luodaan uusi käyttäjätunnus, jos ei ole ennestään, muuten kirjaudutaan sisään vanhalla. Seuraavaksi mennään asetuksiin ja valitaan ”Settings” ja ”Passcode”. Syötetään nelinumeroinen koodi ja vahvistetaan tämä. ”Passcode”-koodia käytetään, kun haluaa pysyä kirjautuneena sisään, mutta jotenkin haluaa suojata pilvipalveluun pääsyn. Seuraavan kerran avaamalla SpiderOak ONE:n, ohjelma kysyy ”Passcode”-tunnusta. Pilvipalveluun tallentamiin tietoihin pääsee käsiksi menemällä asetuksiin ja valitsemalla käyttäjätunnuksesi.

Lopuksi salataan puhelimen muisti käyttäen puhelimen omaa salausmenetelmää. Menään ”Asetukset”, ”Tallennustila ja USB”, ”Puhelimen tallennustila” ja alhaalla ”Puhelimen tallennustilan salaus”. Tarkistetaan, että puhelimin on liitetty seinälaturiin ja akussa on vähintään 80 % varausta. Valitaan ”Seuraava” ja syötetään näytönlukituksen PIN-koodi. Valitaan ”Ota salaus käyttöön”. Jos puhelimessa käytetään SD-muistikorttia, niin tämänkin voi salata menemällä ”Asetukset”, ”tallennustila ja USB”, ”SD-kortti” ja ”Salaa

SD-kortin sisältö”. Valitaan ”Seuraava”, syötetään PIN-koodi ja painetaan ”Ota salaus käyttöön”. SD-kortin salaaminen ei kuitenkaan salaa vanhoja tiedostoja.

6.3 Ulkoiset muistilaitteet

Jos matkailijalla on mukana USB-muistilaite, niin tämä on hyvä turvata. USB-muistitikussa voi salata kansion ja käyttää sitä tai salata koko muistitikun. Ohje on kansion luomiseen, jotta muistitikkua olisi mahdollista käyttää myös salaamattoman. Aloitetaan lataamalla salausohjelma tietokoneelle. Käytän ohjeessa VeraCrypt-salausohjelmaa ja Ubuntu-käyttöjärjestelmää.

Asennetaan VeraCrypt tietokoneelle sivulta ”https://www.veracrypt.fr/en/Downloads.html”. Avataan terminaali ja annetaan komennot: ”cd Downloads”,”tar xvf veracrypt-1.22-setup.tar.bz2”,”./veracrypt-1.22-setup-gui-x64”. Tällöin avautuu viesti, josta valitaan ”Install VeraCrypt”, ”I accept and agree to be bound by the license terms” ja ”OK”. Seuraavaksi avataan ”VeraCrypt” ja ”Create Volume”. Koska salataan koko USB-muistitikku, niin valitaan ”Create a encypted file container” ja painetaan ”Next" ja ”Next”. Valitaan tiedoston sijainti painamalla ”Select File”, valitaan haluamasi paikka salatulle kansiolle, kirjoitetaan nimi, painetaan ”Save” ja ”Next”. Valitaan haluttu salausalgoritmi ”AES(Twofish(Serpent))” ja painetaan ”Next”. Valitaan, kuinka iso kansio halutaan luoda ja ”Next”. Annetaan kansiolle salasana, varmistetaan salasana, painetaan ”Next”, ”Next” ja heilutellaan hiirtä Wizard-ikkunan sisällä, jolloin salaukseen syntyy satunnaisuutta. Painetaan lopuksi ”Format” ja ”OK”. Salattu kansio on valmis. Avatakseen kansio avataan ”VeraCrypt”, painetaan ”Select File..”, valitaan salattu kansio ja painetaan ”Open”. Painetaan ”Slot”-valikosta jotakin numeroa ja painetaan ”Mount”. Seuraavaksi syötetään salasana ja painetaan ”OK”. Hetken jälkeen työpöydälle ilmestyy avattu salattu kansion, jonka sisälle voi siirtää halutut tiedostot.

6.4 Uuden käyttöjärjestelmän asentaminen ja turvaaminen

Esitän ohjeessa, miten Ubuntu-käyttöjärjestelmä asennetaan ja salataan asennuksen aikana. Esitän myös muutaman tietoturvaohjelman asentamisen Ubuntu-käyttöjärjestelmälle. Muut tietoturvaohjelmat voi katsoa otsikon 6.1 Tietokoneen salaa-

minen -kohdan alta. Ubuntu-käyttöjärjestelmän asentamista varten varataan USB-muistilaite, jossa on vähintään 2GB muistia.

Aloitetaan asentaminen lataamalla uusin Ubuntu-käyttöjärjestelmän Desktop-versio täältä ”https://www.ubuntu.com/download/alternative-downloads". Jotta USB-muistitikulta asentaminen onnistuu, se pitää valmistella. Ladataan Etcher tätä varten sivulta ”https://etcher.io/”, joka latautuu zip tiedostona. Puretaan zip valitsemalla se hiiren oikealla näppäimellä ja valitaan kohta "Extract here". Avataan purettu ohjelma, painetaan "Select image", valitaan ISO image ja laitetaan USB-muistitikku tietokoneeseen, jolloin Etcher havaitsee USB-muistitikun automaattisesti. Painetaan ”Flash” ja annetaan tarvittaessa järjestelmävalvojan salasana. Etcherin ollessa valmis, otetaan muistitikku pois ja laitetaan se haluttuun tietokoneeseen kiinni. Käynnistetään tietokone ja mennään BIOS:iin. Tarkistetaan, että tietokone sallii ulkoisilta muistilaitteilta käynnistämisen, ja USB-muistitikulta käynnistäminen on ensimmäinen Boot-listalla. Tässä versiossa tarkistus tapahtuu siirtymällä nuolinäppäimillä Boot-välilehdelle, menemällä USB-muistitikku valinnan päälle ja F6-näppäintä painamalla USB-muistitikulta käynnistäminen on ensimmäinen listalla. Poistutaan painamalla F10-näppäintä ja tallennetaan muutokset. Valitaan kieli ja painetaan ”Install Ubuntu”. Valitaan ”Download updates while installing” ja painetaan ”Continue”. Valitaan ”Erase disk and install Ubuntu” ja ”Encrypt the new Ubuntu installation for security” ja ”Install now”. Valitaan vahva salasana, vahvistetaan se ja painetaan ”Install Now” ja ”Continue”. Valitaan aikavyöhyke, "Continue", näppäimistöstä valitaan Finnish, painetaan "Continue" ja täytetään käyttäjätiedot. Käyttäjätiedoissa valitaan ”Require my password to log in” ja ”Encrypt my home folder”. Asennuksen jälkeen kone on valmis. Tästä lähtien käynnistyksen jälkeen joutuu syöttämään salauksen salasanan, ennen kuin pääsee kirjautumaan sisään. Kun salaus on avattu, Ubuntu-käyttöjärjestelmää voi käyttää normaalisti.

Sähköpostin, selaimen suojaamisen ja WindScriben asentamisen voi katsoa 6.1 Windowsin turvaaminen -kohdan alta. Nämä tietoturvaratkaisut toimivat samalla tavalla Ubuntu-käyttöjärjestelmässä.

Dashlanen tilalle voi asentaa KeePassXC-salasanamanagerin. Avataan terminaali ja annetaan komento ”sudo snap install keepassxc”. Avataan KeePassXC, valitaan ”Create new database” ja ”Save”. Syötetään ja vahvistetaan uusi salasana ja painetaan ”OK”. Uuden salasanan voi lisätä ohjelmaan painamalla ”Add new entry”, syötämällä tiedot ja painamalla ”OK”.

SpiderOakONE asentaminen alkaa avaamalla terminaali ja annetaan komennot "sudo nano /etc/apt/sources.list.d/spideroakone.list" ja "deb http://apt.spideroak.com/ubuntu-spideroak-hardy/ release restricted". Painetaan ctrl+X ja tallennetaan antamalla komento "Y" ja enter. Jatketaan antamalla komennot "sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 573E3D1C51AE1B3D", "sudo apt update", "sudo apt install spideroakone" ja kysymykseen enter. Käyttäjätili toimii samalla tavalla, kuin Windows-osion alla.

6.5 USB-muistitikulta käynnistettävä OS

Ohje on Tails käyttöjärjestelmälle USB-muistilaitteelle. Ohjeessa oleva asennus tapahtuu Ubuntu-käyttöjärjestelmän kautta ja ladataan sivulta ”https://tails.boum.org/install/debian/usb-download/index.en.html”. Samalta verkkosivulta ladataan liitännäinen ja tarkistetaan ladattu tiedosto. Tails-käyttöjärjestelmä on valmiiksi muunneltu turvalliseksi, joten tekemällä asetuksiin muutoksia voi rikkoa turvallisuuden. Verkossa käynti tapahtuu Tor Browser -selaimen kautta. Tor Browser -selaimella on oikeudet lukea ja kirjoittaa vain rajoitetuilla kansioille, joten verkosta lataamisen yhteydessä voi tulla error-ilmoitus. Tor Browser -selain voi ladata vain Tor Browser -kansioon ja kansiossa olevat tiedostot katoavat, kun Tails-käyttöjärjestelmä sammutetaan.

Ensimmäiseksi ladataan uusin ”Tails 3.6.2 ISO image” ja ”Tails Verification”. "Tails verification"-liitännäistä varten sallitaan sen asentua selaimeen, valitsemalla "Allow", "Add" ja "Ok". Tämän jälkeen tarkistetaan ladattu Tails-image, painamalla verkkosivulta ”Verify Tails 3.6.2...”, valitsemalla ISO image ja painamalla open. Verkkosivu tarkistaa, että ladattu Tails-tiedosto on oikea. Tarkistuksen jälkeen painetaan ”Next: Install Tails Installer” ja avataan Ubuntu-käyttöjärjestelmän ohjelma ”Software & Updates”. Avataan ”Other Software”-välilehti ja painetaan ”Add...”-painiketta. APT-kenttään kirjoitetaan ”ppa:tails-team/tails-installer” ja painetaan ”Add Source”, ”Close” ja ”Reload”. Avataan terminaali ja annetaan komento ”apt install tails-installer” ja ”Y”.

Seuraavaksi ladataan muistitikulle Tails. Laitetaan USB-muistitikku koneeseen ja käynnistä Tails Installer. Paina ”None” ja valitse ISO image, joka aikaisemmin ladattiin. Jos automaattisesti valittu USB-muistitikku ei ole se, mihin Tailsin halutaan asentuvan, niin valitaan oikea. Seuraavaksi painetaan ”Install” ja hyväksytään, että kaikki entinen tieto

USB-muistitikussa katoaa painamalla ”Yes”. Tails alkaa asentua muistitikulle ja tässä kestää muutama minuutti. Asentamisen jälkeen syötetään järjestelmävalvojan salasana kahdesti.

Kun asentaminen on saatu loppuun, jätetään USB-muistitikku tietokoneeseen kiinni ja sammutetaan tietokone. Käynnistetään tietokone uudelleen ja varmista, että tietokone sallii USB-muistilaitteelta käynnistämisen ja USB-muistilaite on ensimmäisenä Boot-listalla. Seuraavana tulee esille ”Boot Loader Menu”. Odottamalla hetken Tails käynnistyy automaattisesti. Minuutin odottelun jälkeen ”Tails Greeter” käynnistyy. Tässä voi valita kielen ja näppäimistön. Aloittaaksesi paina ”Start Tails”. Hetken odottelun jälkeen Tails työpöytä tulee näkyviin ja Tails on saatu asennettua.

Seuraavaksi voi luoda valinnaisen salatun ”persistant storage” muistin lopusta USB-muistitikun muistista, jonne voi tallentaa tiedostoja. Tämä vaihtoehto kuitenkin hidastaa huomattavasti Tailsin toimintaa, ”persistant storage” ei ole piilossa ja muuttamalla valmiita asetuksia voi rikkoa tuntemattomana pysymisen. Luodakseen ”persistant storage”, valitaan ”Applications”, ”Tails” ja ”Configure persistant volume”. Annetaan ”Passphrase”, vahvistetaan se ja painetaan ”Create”. Tails aloittaa salaamaan muistia. Painetaan ”Save”. Sammutetaan tietokone ja käynnistetään uudestaan Tails USB-muistitikulta. ”Tails Greeter”-menussa kirjoitetaan ”Encrypted Persistant Storage”-kohtaan valittu ”Passphrase” ja painetaan ”Unlock”. Lopuksi käynnistetään Tails painamalla ”Start Tails”. Nyt voidaan tallentaa yksityistiedot ”Persistant” kansioon, joka löytyy ”Places” ja ”Persistant”.

7 Yhteenveto

Insinöörityössä tutkittiin matkailijalle aiheutuvia tietoturvauhkia. Tavoitteena oli luoda laaja kuva uhista, miten uhkia voi välttää ennen matkalle lähtöä, matkalla ja matkan jälkeen, vertailla eri tietoturvaratkaisuja ja lopuksi rakentaa käytännön ohje tietoturvan parantamiselle.

Työssä selvisi, että tietoturvauhkia on yksityishenkilöiden lisäksi hallitusten virastot, niin suoraan kuin epäsuoraan. Snowdenin paljastuksien perusteella selvisi, että NSA on heikentänyt tahallisesti käytettäviä salausmenetelmiä, ovat luoneet takaovia ja keräävät kaikilta tietoa. Salausten heikentäminen heikentää kaikkien tietoturvaa. Kävi myös sel-

ville, että oikein ja laajasti tehty salaaminen toimii tehokkaasti hyökkääjiä vastaan, ja monet tietoturvauhat ovat matkalla samat, kuin kotimaassa. Matkailija voi varautua näihin kotimaassa käyttämien keinoin. Monet tietoturvaratkaisut ovat helposti asennettavissa ja jokaiselle henkilölle vapaasti käytettävissä.

Olen pyrkinyt parhaani mukaan luomaan laajan ja kattavan tietoturvallisuutta parantavan ohjeen. Ohjeella jokainen pystyy parantamaan omaa tietoturvallisuuttaan tietokoneissa ja puhelimissa ilmaiseksi ja helposti.

Lähteet

1 Yksityisyydensuoja. Verkkoaineisto. <https://www.yksityisyydensuoja.fi/tietoturva>. Luettu 5.4.2018.

2 Raggad, Bel G. 2010. Informaniton Security Management. CRC Press Inc.

3 Bell, James; Borger, Julian & Greenwald, Glen. 2013. Revealed: how US and UK spy agencies defeat internet privacy and security. Verkkoaineisto. The Guardian <https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>. Luettu 10.4.2018.

4 Tossini, J Vitor. 2017. The Five Eyes – The Intelligence Alliance of Anglosphere. Verkkoaineisto. UKDJ <https://ukdefencejournal.org.uk/the-five-eyes-the-intelligence-alliance-of-the-anglosphere/>. Luettu 10.4.2018.

5 2014. Snowden-Interview: Transcript. Verkkoaineisto. NDR <https://www.ndr.de/nachrichten/netzwelt/snowden277_page-3.html>. Luettu 9.4.2018.

6 Vault 7: CIA Hacking Tools Revealed.Verkkoaineisto. WikiLeaks. <https://wikileaks.org/ciav7p1/>. Luettu 12.4.2018.

7 Number of social network users worldwide from 2010 to 2021.Verkkoaineisto. Statista. <https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/>. Luettu 11.4.2018.

8 2018. Cambridge Analytica CEO ‘admits to dirty tricks’. Verkkoaineisto. The Week. <http://www.theweek.co.uk/92390/cambridge-analytica-ceo-admits-to-dirty-tricks>. Luettu 12.4.2018.

9 Frier, Sarah. 2018. Facebook Just Confirmed That It Revies Your Private Messanges. Verkkoaineisto. Times. <http://time.com/money/5227844/facebook-reviews-private-messages/>. Luettu 14.4.2018.

10 2017. Israel, the West Bank and Gaza. Verkkoaineisto. U.S. Department of State. <https://travel.state.gov/content/travel/en/international-travel/International-Travel-Country-Information-Pages/IsraeltheWestBankandGaza.html?wcmmode=disabled>. Luettu 16.4.2018.

11 Blanchard, Ben. 2015. China passes controversial new anti-terrorism law. Verkkoaineisto. Indepent. <https://www.independent.co.uk/news/world/asia/china-passes-controversial-new-anti-terrorism-law-a6787391.html>. Luettu 9.4.2018.

12 Mortleman, Jim. 2009. Top five data security travel issues: Protect sensitive information on business trips. Verkkoaineisto. Computer Weekly. <https://www.computerweekly.com/feature/Top-five-data-security-travel-issues-Protect-sensitive-information-on-business-trips>. Luettu 10.4.2018.

13 Leiva-Gomez, Miguel. 2014. Everything You Need to Know About Fake Cell Towers. Verkkoaineisto. Make tech easier. <https://www.maketecheasier.com/fake-cell-towers/>. Luettu 11.4.2018.

14 Fuzzy. 2016. Turning Your Phone On Is Consenting To Being Tracked. Verkkoaineisto. Deepdotweb. <https://www.deepdotweb.com/2016/02/11/turning-your-phone-on-is-consenting-to-being-tracked/>. Luettu 11.4.2018.

15 2013 Norton Report. Verkkoaineisto. Norton <https://www.symantec.com/about/newsroom/press-kits/norton-report-2013>. Luettu 14.4.2018.

16 Public Wi-Fi Security 101: What makes public Wi-Fi vulnerable to attack and how to stay safe. Verkkoaineisto. Norton. <https://us.norton.com/internetsecurity-wifi-public-wi-fi-security-101-what-makes-public-wi-fi-vulnerable-to-attack-and-how-to-stay-safe.html>. Luettu 14.4.2018.

17 2017. TM testasi: Pankkikortilla tapahtuvasta lähimaksusta löytyi tietoturvauhka – näin voro voi käyttää sitä hyväksi. Verkkoaineisto. Tekniikan maailma <https://tekniikanmaailma.fi/tm-testasi-pankkikortilla-tapahtuvasta-lahimaksusta-loytyi-tietoturvauhka-nain-voro-voi-kayttaa-sita-hyvaksi/>. Luettu 11.4.2018.

18 2017. Lähimaksukorttien turvariskit huolettavat – selvitimme, ovatko kalliit suojakuoret tarpeen. Verkkoaineisto. MTV. <https://www.mtv.fi/uutiset/kotimaa/artikkeli/lahimaksukorttien-turvariskit-huolettavat-selvitimme-ovatko-kalliit-suojakuoret-tarpeen/6432384#gs.gwuduD0>. Luettu 11.4.2018.

19 Grimes, Roger A. 2017. Why you don't need an RFID-blocking wallet. Verkkoaineisto. CSO. <https://www.csoonline.com/article/3199009/security/why-you-dont-need-an-rfid-blocking-wallet.html>. Luettu 11.4.2018.

20 Grimes, Roger A. 2017. The truth about RFID credit card fraud. Verkkoaineisto. CSO. <https://www.csoonline.com/article/3243089/cyber-attacks-espionage/the-truth-about-rfid-credit-card-fraud.html>. Luettu 11.4.2018.

21 Ong, Thuy. 2017. OnePlus is quietly collecting a ton of data from its smartphones. Verkkoaineisto. The Verge. <https://www.theverge.com/circuitbreaker/2017/10/11/16457954/oneplus-phones-collecting-sensitive-data>. Luettu 11.4.2018.

22 Shaikh, Rafia. 2017. Microsoft Comes Clean on Windows 10 Data Collection – Here's Everything Your OS Sends to Redmond. Verkkoaineisto. WCCFtech. <https://wccftech.com/windows-10-data-collection-everything-microsoft-collects/>. Luettu 11.4.2018.

23 Ross, Elizabeth; Decker, J; Lich, Brian & Browser, Nick. 2018. Windows 10, version 1709 basic level Windows diagnostic events and fields, Verkkoaineisto. Microsoft. <https://docs.microsoft.com/en-us/windows/configuration/basic-level-windows-diagnostic-events-and-fields>. Luettu 11.4.2018.

24 Securing the web browser. Verkkoaineisto. F-Secure. <https://www.f-secure.com/en/web/labs_global/browser-security>. Luettu 12.4.2018.

25 Zakas, Nicholas. 2009. Cookies and Security. Verkkoaineisto. NCZOnline. <https://www.nczonline.net/blog/2009/05/12/cookies-and-security/>. Luettu 12.4.2018.

26 Verkkoaineisto. GSMK <http://www.cryptophone.de/en/products/>. Luettu 12.4.2018.

27 Aluminum Foil Does Not Stop RFID. Verkkoaineisto. Omniscience is Bliss. <http://www.omnisciencеisbliss.org/rfid.html>. Luettu 13.4.2018.

28 Electrical systems.Verkkoaineisto. Wikitravel <https://wikitravel.org/en/Electrical_systems>. Luettu 12.4.2018.

29 2016. FACT SHEET: Cybersecurity National Action Plan. Verkkoaineisto. The White House. <https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>. Luettu 13.4.2018.

30 Kun olet ulkomailla. Verkkoaineisto. Danske Bank. <https://danskebank.fi/fi-fi/asiakaspalvelu/henkiloasiakkaat/pages/kun-olet-ulkomailla.aspx>. Luettu 14.4.2018.

31 Howard, Bob. 2010. Telling your bank you are travelling abroad. Verkkoaineisto. BBC. <http://www.bbc.com/news/10351371>. Luettu 14.4.2018.

32 Lee, Micah. 2015. Encrypting Your Laptop Like You Mean It Verkkoaineisto. The Intercept <https://theintercept.com/2015/04/27/encrypting-laptop-like-mean/>. Luettu 14.4.2018.

33 Create a strong password. Verkkoaineisto. Google. <https://support.google.com/accounts/answer/32040?hl=en>. Luettu 15.4.2018.

34 2018. Security Tip. Verkkoaineisto. US-CERT. <https://www.us-cert.gov/ncas/tips/ST04-002>. Luettu 15.4.2018.

35 Dascalescu, Ana. 2017. Here’s How To Get Solid Browser Security [Update 2017]. Verkkoaineisto. Heimdal. <https://heimdalsecurity.com/blog/ultimate-guide-secure-online-browsing/>. Luettu 15.4.2018.

36 2013. Tor is Not as Safe as You May Think. Verkkoaineisto. Info security. <https://www.infosecurity-magazine.com/news/tor-is-not-as-safe-as-you-may-think/>. Luettu 15.4.2018.

37 Palmer, Danny. 2017. Face, fingerprint, passwords, or PIN: What's the best way to keep your smartphone secure?. Verkkoaineisto. ZDNet. <https://www.zdnet.com/article/face-fingerprint-passwords-or-pin-whats-the-best-way-to-keep-your-smartphone-secure/>. Luettu 15.4.2018.

38 3G. Verkkoaineisto. Wikipedia. <https://en.wikipedia.org/wiki/3G#Security>. Luettu 15.4.2018.

39 The Attack Vector “BlueBorne” Exposes Almost Every Connected Device. Verkkoaineisto. Armis. <https://www.armis.com/blueborne/>. Luettu 17.4.2018.

40 Dillet, Romain. 2018. Facebook knows literally everything about you. Verkkoaineisto. Techcrunch. <https://techcrunch.com/2018/03/23/facebook-knows-literally-everything-about-you/>. Luettu 11.4.2018.

41 Whittaker, Zak. 2018. Camera makers resist encryption, despite warnings from photographers. Verkkoaineisto. ZDNet. <https://www.zdnet.com/article/a-year-later-camera-makers-still-resist-encryption/>. Luettu 10.4.2018.

42 2014. Verkkoaineisto. Magic lantern.

<http://www.magiclantern.fm/forum/index.php?topic=10279.msg99214#msg99214>. Luettu 10.4.2018.

43 2014. Verkkoaineisto. <http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html>. Luettu 11.4.2018.

44 Mason, John. 2018. Inside the NSA's War on Internet Security. Verkkoaineisto. Spiegel. <https://thebestvpn.com/are-vpns-legal-banned-countries/>. Luettu 12.4.2018.

45 Kiguolis, Linas. 2018. The Fappening 2018: nudes of Charissa Thompson was leaked. Verkkoaineisto. Tecoreviews. <https://tecoreviews.com/news/fappening-2018-nudes-charissa-thompson-leaked/>. Luettu 10.4.2018.

46 Turner, Karen. 2016. Hacked Dropbox login data of 68 million users is now for sale on the dark Web. Verkkoaineisto. The Washingotn Post. <https://www.washingtonpost.com/news/the-switch/wp/2016/09/07/hacked-dropbox-data-of-68-million-users-is-now-or-sale-on-the-dark-web/?utm_term=.fe3ab34d9a8f>. Luettu 10.4.2018.

47 Linthicum, David. 2014. Clouds are more secure than traditional IT systems -- and here's why. Verkkoaineisto. TechTarget. <https://searchcloudcomputing.techtarget.com/opinion/Clouds-are-more-secure-than-traditional-IT-systems-and-heres-why>. Luettu 11.4.2018.

48 Top 50 Products By Total Number Of "Distinct" Vulnerabilities in 2017. Verkkoaineisto. CVE Details. <https://www.cvedetails.com/top-50-products.php?year=2017>. Luettu 13.4.2018.

49 Operating System Market Share. Verkkoaineisto. Net MarketShare. <https://www.netmarketshare.com/operating-system-market-share.aspx?options=%7B%22filter%22%3A%7B%22%24and%22%3A%5B%7B%22deviceType%22%3A%7B%22%24in%22%3A%5B%22Desktop%2Flaptop%22%5D%7D%7D%5D%7D%2C%22dateLabel%22%3A%22Trend%22%2C%22attributes%22%3A%22share%22%2C%22group%22%3A%22platform%22%2C%22sort%22%3A%7B%22share%22%3A-1%7D%2C%22id%22%3A%22platformsDesktop%22%2C%22dateInterval%22%3A%22Monthly%22%2C%22dateStart%22%3A%222017-04%22%2C%22dateEnd%22%3A%222018-03%22%2C%22segments%22%3A%22-1000%22%7D>. Luettu 13.4.2018.

50 Desktop Operating System Market Share Worldwide. Verkkoaineisto. Statcounter. <http://gs.statcounter.com/os-market-share/desktop/worldwide>. Luettu 13.4.2018.

51 SECURITY REPORT2015/16. Verkkoaineisto. AV-TEST. <https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Security_Report_2015-2016.pdf>. Luettu 14.4.2018.

52 Millman, Rene. 2018. Cortana vulnerability allows hackers to bypass Windows 10 passwords to install malware. Verkkoaineisto. ITPRO. <http://www.itpro.co.uk/security/30732/cortana-vulnerability-allows-hackers-to-bypass-windows-10-passwords-to-install>. Luettu 13.4.2018

53 Taylor, Dave. 2018. Why Linux is better than Windows or macOS for security. Verkkoaineisto. Computerworld.

<https://www.computerworld.com/article/3252823/linux/why-linux-is-better-than-windows-or-macos-for-security.html>. Luettu 9.4.2018

54 Noyes, Katherine. 2010. Why Linux Is More Secure Than Windows. Verkkoaineisto. PCWordld. <https://www.pcworld.com/article/202452/why_linux_is_more_secure_than_windows.html>. Luettu 9.4.2018

55 2017. The State of Open Source Security. Verkkoaineisto. Snyk. <https://snyk.io/stateofossecurity/>. Luettu 11.4.2018

56 Greenberg, Andy. 2014. Verkkoaineisto. <https://www.wired.com/2014/11/protection-from-hackers/>. Luettu 12.4.2018

57 Klosowski, Thorin. 2014. How Splitting a Computer Into Multiple Realities Can Protect You From Hackers. Verkkoaineisto. Wired. <https://lifehacker.com/linux-security-distros-compared-tails-vs-kali-vs-qub-1658139404>. Luettu 12.4.2018.

58 Warren, Tom. 2017. Windows Phone dies today. Verkkoaineisto. The Verge. <https://www.theverge.com/2017/7/11/15952654/microsoft-windows-phone-end-of-support>. Luettu 12.4.2018.

59 Android vs iOS: Which is more secure?. Verkkoaineisto. Norton. <https://us.norton.com/internetsecurity-mobile-android-vs-ios-which-is-more-secure.html>. Luettu 16.4.2018.

60 Mearian, Lucas. 2017. Android vs iOS security: Which is better?. Verkkoaineisto. Computerworld <https://www.computerworld.com/article/3213388/mobile-wireless/android-vs-ios-security-which-is-better.html>. Luettu 16.4.2018.

61 2013. NSA Can Spy on Smart Phone Data. Verkkoaineisto. Spiegel. <http://www.spiegel.de/international/world/privacy-scandal-nsa-can-spy-on-smart-phone-data-a-920971.html>. Luettu 15.4.2018.

62 Ball, James. 2014. Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data . Verkkoaineisto. The Guardian. <https://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data>. Luettu 15.4.2018.

63 Chester, Brandon & Ho, Joshua. 2014. Encyption and Storage Performance in Anroid 5.0 Lollipop. Verkkoaineisto. AnandTech. <https://www.anandtech.com/show/8725/encryption-and-storage-performance-in-android-50-lollipop>. Luettu 14.4.2018.

64 Walters, Geoffrey. 2017. How to Encrypt an iPhone and Add More Security to Your Sensitive Information. Verkkoaineisto. Addictivetips. <https://www.addictivetips.com/ios/encrypt-iphone-tutorial/>. Luettu 14.4.2018.

65 Lee, Micah. 2015. Microsoft Gives Details About Its Controversial Disk Encryption. Verkkoaineisto. The Intercept. <https://theintercept.com/2015/06/04/microsoft-disk-encryption/>. Luettu 14.4.2018.

66 Hoffman, Chris. 2015. What’s the Difference Between BitLocker and EFS (Encrypting File System) on Windows? Verkkoaineisto. How-To Geek.

<https://www.howtogeek.com/236719/whats-the-difference-between-bitlocker-and-efs-encrypting-file-system-on-windows/>. Luettu 14.4.2018.

67 Frisk, Ulf. 2016. macOS FileVault2 Password Retrieval. Verkkoaineisto. <http://blog.frizk.net/2016/12/filevault-password-retrieval.html>. Luettu 13.4.2018.

68 Campbell, Alex. 2016. 3 encryption tools for Linux that will keep your data safe. Verkkoaineisto. PCWorld. <https://www.pcworld.com/article/3140023/linux/3-encryption-tools-for-linux-that-will-keep-your-data-safe.html>. Luettu 13.4.2018.

69 Balducci,Alex; Devlin,Sean & Ritter, Tom. 2015. Open Crypto Audit Project TrueCrypt. Verkkoaineisto. NCCgroup. <https://opencryptoaudit.org/reports/TrueCrypt_Phase_II_NCC_OCAP_final.pdf>. Luettu 13.4.2018.

70 Bedrune, Jean-Daptiste & Videau, Marion. 2016. Security Assessment of VeraCrypt: fixes and evolutions from TrueCrypt. Verkkoaineisto. Quarkslab's blog. <https://blog.quarkslab.com/security-assessment-of-veracrypt-fixes-and-evolutions-from-truecrypt.html>. Luettu 13.4.2018.

71 Alan, Henry. 2013. The Difference Between Antivirus and Anti-Malware (and Which to Use). Verkkoaineisto. Lifehacker. <https://lifehacker.com/the-difference-between-antivirus-and-anti-malware-and-1176942277>. Luettu 12.4.2018.

72 Oramandy, Tavis. 2016. MalwareBytes: multiple security issues. Verkkoaineisto. Chronomium. <https://bugs.chromium.org/p/project-zero/issues/detail?id=714&redir=1>. Luettu 12.4.2018.

73 Scharr, Jill. 2014. Malwarebytes Anti-Malware Free Review. Verkkoainesto. tom's guide. <https://www.tomsguide.com/us/malwarebytes-free,review-2204.html>. Luettu 12.4.2018.

74 Nadel, Brian. 2017. Avira Free Antivirus Review: Less Than Meets the Eye. Verkkoaineisto. tom's guide. <https://www.tomsguide.com/us/avira-free-antivirus,review-2207.html>. Luettu 12.4.2018.

75 Nadel, Brian. 2017. Avast! Free Antivirus Review: Fast, Free and Fun. Verkkoaineisto. Tom's guide. <https://www.tomsguide.com/us/avast-free-antivirus,review-2208.html>. Luettu 12.4.2018.

76 2014. Why Switzerland. Verkkoaineisto. ProtonMail. <https://protonmail.com/blog/switzerland/>. Luettu 12.4.2018.

77 2015. Message Regarding the ProtonMail DDoS Attacks. Verkkoaineisto. ProtonMail. <https://protonmail.com/blog/protonmail-ddos-attacks/>. Luettu 11.4.2018.

78 Copeland, Matthew & Grahn, Joergen & Wheeler, David. Encrypting and decrypting documents. Verkkoaineisto. GnuPG <https://www.gnupg.org/gph/en/manual.html#AEN57>. Luettu 10.4.2018

79 Snowden, Edward. 2015. Verkkoaineisto. Twitter. <https://twitter.com/snowden/status/661313394906161152?lang=fi>. Luettu 12.4.2018.

80 Cohn-Gordon, Katriel; Cremes, Cas; Dowling, Benjamin; Garratt, Luke & Stebila,

Douglas. 2017. A Formal Security Analysis of the Signal Messaging Protocol. Verkkoaineisto. Iacr. <https://eprint.iacr.org/2016/1013.pdf>. Luettu 17.4.2018.

81 Mott, Nathaniel. 2017. Signal's Encrypted Video Calling For iOS, Android Leaves Beta. Verkkoaineisto. Tom's hardware. <https://www.tomshardware.com/news/signal-encrypted-video-calling-ios-android,33898.html>. Luettu 17.4.2018.

82 Signal 2017. Verkkoaineisto. Twitter. <https://twitter.com/signalapp/status/859125874901135360>. Luettu 16.4.2018.

83 Klosowski, Thorin. 2017. Secure Messaging App Showdown: WhatsApp vs. Signal. Verkkoaineisto. Lifehacker. <https://lifehacker.com/secure-messaging-app-showdown-whatsapp-vs-signal-1794684943>. Luettu 15.4.2018.

84 Ludwig, Kelby. End-to-End WhatsApp: An Opinionated Series on Why Signal Protocol is Well-Designed. Verkkoaineisto. Preatorian. <https://p16.praetorian.com/blog/whatsapp-end-to-end-encryption-why-signal-protocol-is-well-designed>. Luettu 16.4.2018.

85 Messieh, Nancy. 2016. How to Stop WhatsApp Handing Your Info to Facebook . Verkkoaineisto. Makeuseof. <https://www.makeuseof.com/tag/how-to-stop-whatsapp-handing-your-info-to-facebook/>. Luettu 16.4.2018.

86 How does Ghostery work?. Verkkoaineisto. Ghostery. <https://www.ghostery.com/faqs/how-does-ghostery-work/>. Luettu 16.4.2018.

87 When does HTTPS Everywhere protect me? When does it not protect me?. Verkkoaineisto. EFF. <https://www.eff.org/https-everywhere/faq#when-does-https-everywhere-protect-me-when-does-it-not-protect-me>. Luettu 17.4.2018.

88 Lauinger, Tobias; Chaabane, Abdelberi; Arshad, Sajjad; Robertson, William & Wilson, Christo. 2017. Thou Shalt Not Depend on Me: Analysing the Useof Outdated JavaScript Libraries on the Web. Verkkoaineisto. Norteastern Univesity. <http://www.ccs.neu.edu/home/arshad/publications/ndss2017jslibs.pdf>. Luettu 17.4.2018.

89 Tor: Overview. Verkkoaineisto. Tor. <https://www.torproject.org/about/overview.html.en>. Luettu 17.4.2018.

90 2013. Tor is Not as Safe as You May Think. Verkkoaineisto. Infosecurity. <https://www.infosecurity-magazine.com/news/tor-is-not-as-safe-as-you-may-think/>. Luettu 15.4.2018.

91 Verkkoaineisto. <https://www.torproject.org/projects/torbrowser.html.en>. Luettu 15.4.2018.

92 Athow, Desire. 2017. Why you need a VPN when browsing on public Wi-Fi. Verkkoaineisto. Techradar. <https://www.techradar.com/news/public-wi-fi-and-why-you-need-a-vpn>. Luettu 14.4.2018

93 Verkkoaineisto. Windscribe. <https://windscribe.com/upgrade>. Luettu 12.4.2018.

94 Crawford, Douglas. 2013. Tor vs. VPN. Verkkoaineisto. BestVPN. <https://www.bestvpn.com/tor-vs-vpn/>. Luettu 13.4.2018.

95 OpenVPN Community Software. Verkkoaineisto. OpenVPN. <https://openvpn.net/index.php/open-source/333-what-is-openvpn.html>. Luettu 16.4.2018.

96 Bevad, Marc. 2016. My Experience With the Great Firewall of China. Verkkoaineisto. Mrb's blog. <http://blog.zorinaq.com/my-experience-with-the-great-firewall-of-china/>. Luettu 17.4.2018.

97 Heiderich, Mario. 2017. TunnelBear Security Assessment Summary 07.2017. Verkkoaineisto. Cure53. <https://cure53.de/summary-report_tunnelbear.pdf>. Luettu 17.4.2018.

98 Paul, Ian. 2017. TunnelBear review: If you can stand the puns, TunnelBear is a speedy VPN. Verkkoaineisto. PCWorld. <https://www.pcworld.com/article/3201008/privacy/tunnelbear-vpn-review.html>. Luettu 13.4.2018.

99 2018. Windscribe VPN Review: The Cold Hard Facts You Need To Read Right Now. Verkkoaineisto. SecurityGladiators. <https://securitygladiators.com/windscribe-vpn-review/>. Luettu 12.4.2018.

100 Paul, Ian. 2014. Edward Snowden: Dropbox is 'hostile to privacy'. Verkkoaineisto. PCWorld. <https://www.pcworld.com/article/2455215/edward-snowden-dropbox-is-hostile-to-privacy.html>. Luettu 15.4.2018.

101 2017. Why We Will No Longer Use the Phrase Zero Knowledge to Describe Our Software. Verkkoaineisto. SpiderOak. <https://spideroak.com/articles/why-we-will-no-longer-use-the-phrase-zero-knowledge-to-describe-our-software/>. Luettu 14.4.2018.

102 Hoffman, Chris. 2015. Tails 1.4 polishes up the privacy-obsessed Linux OS trusted by Edward Snowden. Verkkoaineisto. PCWorld. <https://www.pcworld.com/article/2923013/tails-14-polishes-up-the-privacy-obsessed-linux-os-trusted-by-edward-snowden.html>. Luettu 13.4.2018.

103 Qubes Live USB (alpha). Verkkoaineisto. Qubes. <https://www.qubes-os.org/doc/live-usb/>. Luettu 15.4.2018.

104 Verkkoainesto. Tails. <https://tails.boum.org/doc/about/warning/index.en.html>. Luettu 16.4.2018.

105 2014. Snowden-Interview: Transcript. Verkkoaineisto. NDR. <https://www.ndr.de/nachrichten/netzwelt/snowden277_page-3.html>. Luettu 16.4.2018.

106 Gentili, Paolo & Shader, Sarah & Yip, Richard & Zeng, Brandon. 2016. Security Analysis of Dashlane. Verkkoaineisto. MIT. <https://courses.csail.mit.edu/6.857/2016/files/25.pdf>. Luettu 16.4.2018.

107 2016. KeePass Password Safe. Verkkoaineisto. European Commission. <https://joinup.ec.europa.eu/sites/default/files/inline-files/DLV%20WP6%20-01-%20KeePass%20Code%20Review%20Results%20Report_published.pdf>. Luettu 16.4.2018.

108 Lurey, Craig. 2017. Update for Keeper Browser Extension 11.4.4. Verkkoaineisto. Keeper. <https://keepersecurity.com/blog/2017/12/15/update-for-keeper-browser-

extension-v11-4/>. Luettu 16.4.2018.