Osaamista
ja oivallusta
tulevaisuuden
tekemiseen

Vili Länsiharju, Pihla Mattila

Yksityisyys ja seuranta verkossa

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

18.11.2018

Tekijä Otsikko Sivumäärä Aika	Vili Länsiharju, Pihla Mattila Yksityisyys ja seuranta verkossa 51 sivua + 1 liite 18.11.2018
Tutkinto	Insinööri (AMK)
Tutkinto-ohjelma	Tietotekniikan koulutusohjelma
Ammatillinen pääaine	Tietoverkot
Ohjaajat	Lehtori Marko Uusitalo

Insinöörityön tarkoituksena oli selvittää, millä eri tavoin ihmisiä seurataan internetissä ja miten tältä seurannalta voi suojautua. Asiaan tutustuminen aloitettiin perehtymällä viime aikojen suurimpiin tietovuotoihin ja siihen, miten ne ovat vaikuttaneet näkemyksiin yksityisyydestä. Seurannan menetelmistä tutkittavia aiheita oli muun muassa selaimen jättämä sormenjälki, pikseliseuranta ja sosiaalisen median kautta suoritettava seuranta. Yksityisyyden suojaamisen menetelmistä perehdyttiin yleisempiin keinoihin, kuten VPN-palveluihin ja Tor-verkon toimintaan.

Insinöörityön tavoitteena oli luoda kattavat ohjeet yksityisyyden suojaamiseksi internetissä. Lisäksi suunniteltiin ja rakennettiin kotiverkon suoja seurantaa vastaan. Tämä toteutettiin asentamalla mainonnan- ja seurannanestopalvelu Pi-hole Raspberry Pi:lle. Kotiverkon suojaa laajennettiin asentamalla OpenVPN-palvelin, jotta suojatun verkon käyttö onnistuisi myös etäyhteyksillä. Verkon suorituskykyä mitattiin erilaisilla menetelmillä.

Insinöörityössä havaittiin, että tavallisen käyttäjän on lähes mahdotonta pysyä täysin anonyyminä internetissä, mutta tapoja parantaa yksityisyydensuojaa löytyy. Tärkeäksi havainnoksi nousi myös, että on tärkeää pitää kiinni oikeudestaan yksityisyyteen maailmassa, jossa jatkuva seuranta on yhä yleistyvämpää.

Kotiverkon suojaamisessa onnistuttiin odotusten mukaisesti. Suorituskykymittauksista kävi ilmi, että VPN-palvelimen käyttö hidasti yhteyksiä jonkin verran, mutta tavallinen internetin käyttö onnistui normaalisti satunnaisia käyttökatkoja 3G-yhteyksillä lukuun ottamatta.

Avainsanat	yksityisyys, seuranta, VPN, DNS

Author Title Number of Pages Date	Vili Länsiharju, Pihla Mattila Online Privacy and Tracking 51 pages + 1 appendix 18 November 2018
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Professional Major	Data Networks
Instructors	Marko Uusitalo, Senior Lecturer

The purpose of this thesis was to examine the different ways people are tracked across the internet and how it is possible to prevent such tracking. This thesis goes over some of the major data leaks of recent years and the ways they have affected the way privacy issues are seen today.

The goal of this thesis was to provide a comprehensive list of suggestions for staying private on the internet and instructions for securing network traffic of a user from tracking. This was done by configuring a DNS server with Raspberry Pi. Further protection is achieved by installing a VPN-server for mobile usage.

The conclusion of this thesis was that for a normal user it is not possible to stay completely anonymous on the internet but there are multiple ways for improving privacy. It is also crucial for people to stay on top of things when it comes to privacy issues in a world where it is becoming a norm that everyone is being watched all the time.

Keywords	Privacy, Tracking, VPN, DNS

Sisällys

Lyhenteet

GDPR	Euroopan Unionin yleinen tietosuoja-asetus, 2016/679.
VPN	*Virtual Private Network.* Virtuaalinen erillisverkko.
UDP	*User Datagram Protocol.* Yhteydetön kuljetusprotokolla.
DNS	*Domain Name System.* Internetin nimipalvelujärjestelmä, joka muuntaa verkkotunnuksia IP-osoitteiksi.
EFF	*Electronic Frontier Foundation.* Kansainvälinen tietoyhteiskunnan kansalaisoikeuksia puolustava järjestö.

1 Johdanto

Tämän insinöörityön tarkoituksena on tutkia, millä eri tavoin henkilöä seurataan internetissä ja miten oikeus yksityisyyteen toteutuu. Tavoitteena on löytää ratkaisuja, miten tältä seurannalta voi suojautua. Insinöörityön on tarkoitus toimia kattavavana tietopakettina, jossa käydään läpi eri seurannan menetelmiä ja neuvotaan, miten seurannalta voi suojautua.

Insinöörityössä tutkitaan eri vaihtoehtoja oman internetliikenteen suojaamiseksi ja suunnitellaan lisäsuoja kotiverkolle sekä siihen liitetyille laitteille. Työn lopuksi tehdään suorituskyvyn mittauksia laitteistolla. Työ toteutetaan pienoistietokone Raspberry Pi:llä sen pienten kustannusten sekä pienen virrankulutuksen takia. Raspberry Pi:lle asennetaan verkkotason mainonnan- ja seurannanestopalvelu Pi-hole. Verkkotason suojaa laajennetaan OpenVPN-palvelimen asennuksella, joka mahdollistaa verkkoliikenteen suojaamisen myös kotiverkon ulkopuolella.

Seurantaa harrastetaan usein tarkoituksenmukaisesti, mutta sillä saattaa myös olla pahantahtoisia tarkoitusperiä. Sen takia raportissa esitellään joitakin tietoturvarikollisten harjoittamia tiedonkeruumenetelmiä, jotka myös luovat uhan yksityisyydelle. Tieto on nykypäivänä erittäin arvokasta ja siitä hyötyvät niin yritykset, valtiot ja yksityishenkilöt.

> *“You have zero privacy anyway. Get over it.”* Scott McNealy, Sun Microsystemsin toimitusjohtaja, 1999 [1, s. 14]

Seurantaa tapahtuu koko ajan, kaikkialla. Viime vuosina yhdeksi yhteiskunnan tärkeimmäksi kysymykseksi onkin noussut yksityisyydensuoja. Ympäri maailmaa on paljastunut toinen toistaan häikäilemättömämpiä tapauksia, joissa ihmisten tekemisiä on tarkkailtu ja tietoja on tallennettu sekä käytetty ilman suostumusta. Scott McNealyn vuonna 1999 lausuma synkkä mielipide on ehkä nykyään vielä ajankohtaisempi kuin kaksi vuosikymmentä sitten. Yksityisyydensuojan heikentyminen on valitettava totuus nyky-yhteiskunnassa, mutta se ei tarkoita, etteikö sitä vastaan voisi taistella.

Yleensä valtioiden harjoittamaa seurantaa perustellaan turvallisuudella ja aiheesta puhuttaessa kuuleekin usein jo kuluneen väitteen: ”Minulla ei ole mitään salattavaa, koska

en tee mitään kiellettyä.” Väite on harvoin totta, sillä kukapa olisi valmis julkaisemaan esimerkiksi henkilökohtaiset Google-haut, tiliotteet ja sähköpostit. Vaikka näitä tietoja säilytettäisiin turvallisesti, täytyy muistaa, että ne voivat aina joutua myös vääriin käsiin.

Seurannan ja tiedonkeruun laajuutta on vaikea käsittää, sillä se on pikkuhiljaa tullut osaksi jokapäiväistä elämää. Älypuhelinten ja sosiaalisen median aikakausi on tuonut mukanaan elämäntavan, jossa ihminen on koko ajan yhteydessä internetiin ja näin ollen jatkuvan tiedonkeruun kohteena. Kaikki tiedonkeruu ei tietenkään ole harmillista, ja se on usein jopa välttämätöntä palveluiden toiminnan takaamiseksi. Tarkemmin sanottuna tiedonkeruu itsessään ei ole ongelma, vaan se, miten tietoja käsitellään, mihin sitä käytetään ja kenellä on pääsy niihin.

2 Yksityisyyden tilanne nykypäivänä

2.1 Cambridge Analytica -skandaali

Ehkä kaikkien aikojen suurin tietovuoto paljastui maaliskuussa 2018, kun selvisi, että Cambridge Analytica -niminen yritys oli väärinkäyttänyt miljoonien ihmisten Facebook-profiileja. Cambridge Analytica loi algoritmin, jolla se pystyi ennustamaan ihmisten käyttäytymistä Brexit-äänestyksessä ja USA:n presidentinvaaleissa. Alkuperäinen data kerättiin persoonallisuustestisovelluksella, thisisyourdigitallife, jolle käyttäjät antoivat luvan käyttää tietojaan tieteelliseen tutkimukseen. Sovellus kuitenkin keräsi luvatta myös käyttäjien Facebook-kavereiden tietoja, jolloin lopullinen profiilien määrä nousi kymmeniin miljooniin. Tämä oli Facebookin ehtojen vastaista, mutta sitä ei ollut estetty millään tavalla. Tietojen avulla yhtiö kehitti ohjelman, jolla pystyi profiloimaan äänestäjiä ja näyttämään heille kohdennettuja mainoksia, joilla vaikutettiin äänestyskäyttäytymiseen.

Facebook on myöntänyt, että se tiesi tietovuodosta jo vuonna 2015, jolloin se poisti sovelluksen ja vaati Cambridge Analyticaa poistamaan sovelluksen keräämät tiedot. Uutistoimistot The Guardian ja The New York Times ovat myöhemmin saaneet selville, että tietoja ei ollut poistettu. [2.]

Skandaalin jälkeen kolme miljoonaa eurooppalaista käyttäjää jätti palvelun, ja Facebookin osake menetti arvostaan lähes 20 %. Facebookin käyttäjien lukumäärä on kohusta huolimatta jatkanut kasvuaan, tosin hitaammin kuin ennen skandaalia. [3.]

Facebook on yrittänyt korjata tilannetta muutoksilla, joiden on tarkoitus parantaa käyttäjien yksityisyyttä ja tietoturvaa. Se on tiukentanut kolmannen osapuolen sovellusten valvontaa, päivittänyt yksityisyysasetuksia ja alkanut vaatimaan poliittisilta mainostajilta todistuksen henkilöllisyydestä. Lisäksi Facebook on ilmoittanut keskittyvänsä entistä paremmin väärän ja virheellisen tiedon leviämisen estämiseen poistamalla epäilyttäviä sivuja, ryhmiä ja käyttäjiä. [4.]

2.2 NSA-vakoiluskandaali

Vuonna 2013 Yhdysvaltain keskustiedustelupalvelun CIA:n entinen työntekijä Edward Snowden toi julkisuuteen useita maailmanlaajuisia joukkovalvontasuunnitelmia. Yhdysvaltojen kansallinen turvallisuusvirasto NSA oli käyttänyt terrorismin vastaiseen taisteluun suunniteltua PRISM-tietokoneohjelmaa verkkoliikenteen keräämiseen ja tallentamiseen vuodesta 2007 lähtien. Sillä oli pääsy mm. Microsoftin, Googlen, Facebookin ja Applen palvelimille ja sitä kautta yksityisten henkilöiden sähköposteihin, kuviin ja videoihin. Lisäksi tietoliikenneyritys Verizonin miljoonien asiakkaiden puhelutietoja oli kerätty. Samalla paljastui, että myös brittiläisellä tiedustelu- ja turvallisuuspalvelu GCHQ:lla (Government Communications Headquarters) oli pääsy maansa kansalaisten vastaaviin tietoihin. [5.]

Yhdysvallat, Britannia, Kanada, Australia ja Uusi-Seelanti muodostavat viiden maan yhteisen tiedusteluliiton, jota kutsutaan nimellä Five Eyes (FVEY). Suuri osa paljastetuista dokumenteista oli suunnattu tämän liiton jäsenille. Edward Snowden on sanonut liiton toimivan omien maidensa lakien tavoittamattomissa, sillä vaikka ne eivät suoraan vakoilisikaan omia kansalaisiaan, se ei tarkoita, etteivätkö ne pääsisi tietoihin käsiksi tiedonjaon kautta.

Paljastusten jälkeen näytti siltä, että tiedustelulakeihin tulisi muutoksia, mutta viisi vuotta tapahtumien jälkeen muutokset ovat jääneet osittain pintapuolisiksi. Yhdysvaltojen Freedom Act estää NSA:ta keräämästä puhelutietoja, mutta Trumpin hallinto antoi tänä vuonna sille luvan vakoilla muiden maiden kansalasten telekommunikaatiota. EU:n yleisen tietosuoja-asetuksen GDPR:n sanotaan saaneen vauhtia ja näkyvyyttä skandaalista. [6.]

2.3 Kiinan verkkovalvonta

Kiinan hallituksen tavoite on vuoteen 2020 mennessä pystyä valvomaan aukottomasti kaikkea, mitä sen kansalaiset tekevät. Kiinassa arvioidaan tällä hetkellä olevan noin 180 miljoonaa valvontakameraa ja kameroiden määrää tullaan nostamaan arvioiden mukaan

626 miljoonaan asti. Jatkuvan kameravalvonnan lisäksi kiinalaisia vahditaan tekoälyn avulla, joka tunnistaa jo yli 90 prosenttia kameroiden kuvaamista henkilöistä.

Osa Kiinan verkkokontrollia on kaiken internetliikenteen valvonta. Valtionlaajuinen palomuuri estää kiinalaisten pääsyn sivustoille ja sovelluksiin, jotka hallinto katsoo haitallisiksi. Kiellettyjä sivustoja ovat mm. Facebook, YouTube ja Twitter. VPN-palvelun käyttöä ei ole kielletty laissa suoranaisesti, mutta hallinto tekee jatkuvasti tehoiskuja palvelinten sulkemiseksi.

Vuonna 2014 julkaistiin suunnitelma kansalaisten sosiaalisesta pisteyttämisestä (social credit). Järjestelmän on tarkoitus tulla täysivoimaisesti käyttöön vuonna 2020, ja sen kokeilu aloitettiin vuoden 2018 toukokuussa. Pisteytyksen tarkoituksena on kertoa, kuinka kunnollinen ihminen on. Muun muassa rikokset ja paheksuttavat harrastukset kuten tietokoneella pelaaminen vaikuttavat pisteisiin negatiivisesti. Pistemäärään voi vaikuttaa myös sopimattomien poliittisten mielipiteiden ilmaisu ja huonoksi katsottava toiminta verkossa. [7.]

Kiinan tiukka verkkovalvonta on herättänyt kiinnostusta myös maailman muissa vähemmän demokraattisissa maissa. Osana digitaalista silkkitietä eli Kiinan voimakasta pyrkimystä levittää teknologiaosaamistaan maailmalle, on kiinalainen televiestintälaitteiden valmistaja Huawei rakentamassa ympäri maailmaa älykaupunkeja, joita markkinoidaan turvallisuudella ja teknologisella edistyksellisyydellä. Kehittyvissä maissa ei välttämättä löydy omaa it-osaamista, jolloin niiden on helppo kääntyä kiinalaisen yhteistyökumppanin puoleen. Tämä mahdollistaa teknologian lisäksi Kiinan ideologian leviämisen, jonka mukaan tiedon vapaa liikkuminen nähdään uhkana. [8.]

Huawei on ollut Suomessakin vahvasti mukana verkkohankkeissa, ja se on mm. toimittanut Ukkoverkot Oy:lle maailman ensimmäisen kaupallisen 450 MHz LTE-verkon. [9.]

2.4 Tilanne Suomessa

Viime vuosien terroriteot ovat herättäneet huolta kansallisesta turvallisuudesta ja Suomessa on valmisteltu viranomaisten tiedusteluoikeuksien laajentamista tällä perusteella.

Uusi tiedustelulaki halutaan voimaan mahdollisimman nopeasti, mutta nykyinen perustuslaki ei salli viestisuojan rikkomista kansallisen turvallisuuden perusteella. Tämän johdosta eduskunta äänesti kiireellisestä perustuslakimuutoksesta, jolla perustuslaki saadaan muutettua jo kuluvalla vaalikaudella, kun yleensä perustuslakimuutos tehdään kahden vaalikauden aikana.

Uusi laki antaisi Suomen sotilastiedustelulle ja Suojelupoliisille yleisen pääsyn Suomen rajat ylittäviin tietoliikennekaapeleihin, mikä käytännössä mahdollistaisi joukkovalvonnan. Joukkovalvontaa ei kuitenkaan aiota sallia, vaan tiedustelu on tehtävä mahdollisimman kohdennetusti ja vain tuomioistuimen luvalla. Lisäksi tiedustelulaki toisi muutoksen, jonka avulla toimivaltuudet laajentuisivat koskemaan myös sellaisen toiminnan tiedustelua, missä ei ole havaittu selkeää rikosta, kun nykyisin tiedustelulupaan tarvitaan näyttö jo tapahtuneesta rikoksesta.

Suomessa poliisi nauttii syvää luottamusta huolimatta siitä, että on käynyt ilmi useita toimivaltuuksien väärinkäytöksiä. Vuonna 2014 tuomittiin yli 70 poliisin henkilökuntaan kuuluvaa henkilöä Mika Myllylän kuolinsyyn urkinnasta. Lisäksi Anneli Auerin ja Jari Aarnion tapauksien tietoja on katseltu luvattomasti useiden kymmenien poliisien toimesta. [10.]

Helsingin Sanomien vuonna 2014 tekemän selvityksen mukaan varsinkin Helsingin poliisille ja Helsingin huumepoliisille myönnettyjen teletietojen ja puhelinkeskustelujen seurannan lupien hakemuksissa esiintyi paljon puutoksia. Hakemukset olivat ylimalkaisia ja niistä puuttuivat perustelut sekä yksityiskohdat, miksi poliisi epäilee jonkun tietyn puhelimen käyttäjää. Puutteista huolimatta luvat myönnettiin aina. Myös Helsingin käräjäoikeuden päätökset olivat usein niin huonosti perusteltuja, että salaisten pakkokeinojen käyttöä on jälkikäteen mahdotonta valvoa.

Suomessa on havaittu todelliseksi ilmiöksi salaisen tiedonhankinnan porttiteoria, jonka mukaan kerran poliisille myönnetty valtuus alkaa laajeta koskemaan suurempaa kansalaisten yksityiselämän suojan ja perusoikeuksien osaa. Myönnetyt valtuudet synnyttävät rinnalleen uusia valtuuksia, jotka myös alkavat laajeta tahoillaan. [11.]

2.5 Google

Google on maailman suurin yksittäinen tiedonkerääjä. Se voi tallentaa kirjautuneen käyttäjän verkko- ja sovellustoiminnan, eli sivustot, joilla kävijä vierailee, käytetyt hakusanat jne. Lisäksi se voi tallentaa käyttäjän sijaintihistorian, yhteystiedot ja kalenterimerkinnät. Myös puhetta ja ääntä tallennetaan. Puheen tallennus tapahtuu, kun Googlea käytetään puheohjauksella. Googlen haku herää sanoihin ”Okei Google” ja sen jälkeen haku käynnistyy, jolloin kaikki puhe ja ääni tallennetaan. Lisäksi se tallentaa YouTuben haku- ja katseluhistorian, eli kaikki videot, joita käyttäjä on katsonut ja minä päivänä ne on katsottu. Lisäksi on mahdollista antaa sille lupa luovuttaa tiedot kolmannen osapuolen sovelluksille.

Vaikka ei käyttäisi Googlen tuotteita, eikä Googlen hakukonetta, sillä on pääsy käyttäjän tietoihin muiden sivustojen kautta. Monet sivustot käyttävät Google Analytics -työkalua kävijöiden analysointiin. Vaikka ei itse käyttäisi Googlen sähköpostia, sillä on pääsy kaikkiin niihin sähköposteihin, jotka lähetetään Gmailia käyttäville henkilöille.

Googlen tiedetään seuranneen käyttäjien sijaintia, vaikka sijaintipalvelut oli kytketty pois päältä. On myös paljastunut, että se on seurannut Android-puhelimien käyttäjiä keräämällä lähellä olevien tukiasemien osoitteita. [12.]

Vuonna 2010 saksalaisen tietosuojavaltuutetun tarkastuksen yhteydessä Google joutui myöntämään, että sen Street View -autot olivat keränneet langattomien lähiverkkojen tietoja vuodesta 2007 lähtien. Autot olivat keränneet SSID-tietoja sekä MAC-osoitteita havaitsemistaan verkoista. Lisäksi paljastui, että autot olivat keränneet myös suojaamattomissa verkoissa liikkunutta dataa, mm. valokuvia, käyttäjänimiä, sähköposteja ja muita dokumentteja. Aluksi Google väitti, ettei se tiennyt asiasta ja syynä tietojen keräämiseen oli kokeellisessa koodinpätkässä, joka oli vahingossa päätynyt lopulliseen ohjelmakoodiin. Myöhemmin kuitenkin kävi ilmi, että tieto datan keräämisestä oli ollut tiedossa. [13; 14.]

Syksyllä 2018 paljastui, että Google on valmistelemassa hakukonetta Kiinan markkinoille. Dragonfly-koodinimellä kutsutun hakukoneen on tarkoitus sensuroida julkaisuja, joissa käsitellään sananvapautta, ihmisoikeuksia, demokratiaa ja muita Kiinan hallinnon

mielestä sopimattomia aiheita. Lisäksi se yhdistää hakuhistorian käyttäjän puhelinnumeroon. [15.]

2.6 GDPR

EU:n yleinen tietosuoja-asetus GDPR (General Data Protection Regulation) on Euroopan unionin yksityisyyslaki. GDPR yhtenäistää henkilökohtaisten tietojen käsittelyn EU-maiden kesken. Tietosuoja-asetus hyväksyttiin 27.4.2016, ja se astui voimaan kahden vuoden siirtymäajan jälkeen 25.5.2018. Sen tarkoituksena on turvata EU-kansalaisten henkilötietoja ja niiden käsittelyä niin EU:n sisällä kuin ulkopuolella. Lisäksi se antaa kansalaiselle oikeuden tarkistaa hänestä tallennetut tiedot sekä mistä tiedot on saatu ja onko niitä jaettu eteenpäin. Asetus korvaa aiemman, vuonna 1995 voimaan astuneen, EU:n tietosuojadirektiivin (European Data Protection Directive).

Tietosuoja-asetus määrää, että kuluttajalla on oikeus tarkistaa ja siirtää omat tietonsa rekisterinpitäjältä toiselle, jos se on teknisesti mahdollista. Kuluttajalla on ennenkin ollut oikeus saada tietonsa rekisterinpitäjältä, mutta entinen kolmen kuukauden vastausaika on lyhentynyt kuukauteen. Jos kuluttaja pyytää tietonsa sähköisesti, ne on toimitettava sähköisesti, ja jos sähköinen toimitus ei onnistu, tiedot on toimitettava paperisena.

GDPR koskee kaikkia osapuolia, jotka ovat joko suoraan tai välillisesti mukana yksityishenkilön tietojen käsittelyssä. Esimerkkinä voi ajatella yritystä, joka tarjoaa pilvipalveluratkaisuja asiakkailleen. Jos pilvipalvelun mukana käytetään alihankkijan kehittämää ohjelmaa tai työkalua, jolla kerätään tietoa asiakkaasta, niin GDPR koskee niin yritystä kuin myös mahdollista alihankkijaa, mikä velvoittaa molemmat osapuolet käsittelemään henkilötietoja tietosuoja-asetuksen mukaisesti.

GDPR määrittää henkilökohtaisten tietojen suojaamista eri salausmenetelmillä, kuten pseudonymisaatiolla. Pseudonymisaatio tarkoittaa tiettyyn henkilöön yhdistettävissä olevien henkilötietojen korvaamisen esimerkiksi numerotunnisteella tai salanimellä, jolloin henkilötietoja ei suoraan voi yhdistää henkilöön. GDPR:n määrityksessä EU-kansalaisen yksityisyyttä koskeviin tietoihin lukeutuu tavallisten henkilötietojen (nimi, sosiaaliturvatunnus, osoite ja sähköposti) lisäksi henkilön verkkotiedot (IP-osoite, sijainti, evästetiedot

ja RFID-tunniste). Henkilökohtaisiin tietoihin luetaan myös yksityishenkilön terveyteen liittyvät tiedot, poliittiset näkemykset sekä seksuaalinen suuntautuminen.

Asetuksessa määritetään myös mahdolliset sanktiot ehtojen rikkomisesta, jotka ovat korkeimmillaan 20 miljoonan euron sakko tai neljä prosenttia edeltävän tilikauden maailmanlaajuisesta liikevaihdosta riippuen tiedonkerääjän koosta. Sakko määräytyy sen mukaan, kumpi näistä luvuista on suurempi. Mahdollisen tietomurron yhteydessä GDPR velvoittaa tiedonkerääjää ilmoittamaan asiasta asiakkaalle 72 tunnin sisällä. [16.]

3 Seurannan menetelmiä

3.1 Selaimen sormenjälki

Selaimen sormenjäljellä tarkoitetaan selaimesta saatavaa tietoa, jonka avulla sivustot voivat seurata käyttäjää eri sivustoilla ja rakentaa käyttäjästä profiilin mainontaa varten. Tämä tarkoittaa käyttäjän selainasetusten sekä käyttöympäristön seurantaa, johon kuuluvat esimerkiksi näytön asetukset, asennetut fontit sekä selaimen lisäosat. Jos käyttäjä vierailee tietyllä sivustolla, on suuri mahdollisuus, että seuraavan kerran käyttäjän vieraillessa samalla sivustolla, sivusto tunnistaa käyttäjän, vaikka tämä olisi poistanut evästeet ja käyttäisi esimerkiksi VPN-yhteyttä. Selaimen sormenjälkitunnistus on hyvin suosittu tapa kerätä käyttäjästä tietoa, koska toisin kuin evästeet, se ei vaadi esimerkiksi mitään tietoa tallennettavaksi käyttäjän koneille. Tämän takia siltä on hyvin vaikea suojautua. [17.]

Hyvänä esimerkkinä käyttäjien selaimen seurannasta ja siihen kohdistuvasta mainonnasta voidaan pitää matkailusivusto Orbitzin harjoittamaa tapaa. Vuonna 2012 Orbitz laskutti hotellien huonevarauksista 20-30 dollaria enemmän, jos käyttäjä teki varauksen Applen laitteilla. Orbitz puolustautui sanomalla kyseessä olevan pelkästään kokeilu ja on sittemmin perunut kyseisen laskutuskäytännön. [18.] Toinen esimerkki on Wall Street Journalin käyttöönottama maksumuuri, joka määräytyy jokaiselle ei-tilaajalle henkilökohtaisesti. Sen on määrä tunnistaa, kuinka todennäköisesti satunnainen lukija tekee tilauksen lehteen ja sisältöä näytetään sen mukaan. Jokaiselle ei-tilaajalle lasketaan arvosana erilaisten indikaattorien mukaan, kuten käyttöjärjestelmä, laite, sijainti ja vieraillaanko sivulla ensimmäistä kertaa. [19.]

Isoimman tietoturvan selaimen sormenjäljen tunnistamisessa luo JavaScript, jonka avulla pystyy selvittämään usean eri selaimen ohjelmointirajapintojen avulla paljon tarkempaa tietoa käyttäjästä. JavaScriptin avulla sivustot voivat saada selville käyttöjärjestelmälle asetetun aikavyöhykkeen, joka voi olla esimerkiksi VPN:n käyttäjälle ongelmallista. On myös monia muita ongelmallisia ohjelmointirajapintoja, joita voidaan käyttää tiedon keräämiseen. Näistä mainitsemisen arvoisia ovat Canvas-, WebGL- ja AudioContext-rajapinnat.

Canvas-sormenjälkitunnistuksessa (Canvas fingerprinting) käyttäjälle annetaan selaimessa mallinnettavaksi kuva. Tällä tavoin saadaan esitysalueen tuottama pikselidata, jonka jälkeen datasta saadaan luotua tarkiste (hash), joka toimii sormenjälkenä. Koska mallinnettava kuvan erot riippuvat käytetystä selaimesta, käyttöjärjestelmälle asennetuista fonteista, käyttäjän käyttämästä näytönohjaimesta sekä näytönohjaimelle asennetun ajurin versiosta, on pikselidatasta saatu tarkiste lähes ainutlaatuinen. [20; 21.]

WebGL (Web Graphics Library) on JavaScriptiä käyttävä ohjelmointirajapinta, jolla mallinnetaan 2D- ja 3D-grafiikkaa verkkoselaimelle. Vaikka sen avulla saadaan tietoa käytettävästä näytönohjaimesta, isompana turvallisuusriskinä pidetään rajapinnan mahdollisuutta ajaa koodia suoraan näytönohjaimella. Tämä tarkoittaa, että sivustot pääsevät käsiksi näytönohjaimen omiin rajapintoihin, joita ei ole suunniteltu varsinaisesti turvallisuusmielessä. Mahdollisia hyökkäyksiä käyttäjän koneelle voidaan tulevaisuudessa toteuttaa WebGL-rajapintaa hyödyntäen. [22.]

Audiocontext-sormenjälkitunnistuksessa (AudioContext fingerprinting) hyödynnetään selaimista löytyvää Audiocontext-rajapintaa, jolla tuotetaan kiinteitä ääniaaltomuotoja, kuten sini- tai kolmioaalto. Tällä tavalla pystytään huomaamaan pieniä eroavaisuuksia äänen mallinnuksessa, josta luodaan sormenjälkitunniste. [23.]

Yksi vähemmän tunnettu haavoittuvuus on WebRTC (Web Real-Time Communication). WebRTC on avoimen lähdekoodin ohjelmointirajapinta, joka mahdollistaa reaaliaikaiset yhteydet kuten ääni- ja videopuhelut, suoratoiston ja vertaisverkkoyhteydet kahden selaimen välille ilman selainlaajennosta. Kahden WebRTC:n kautta suoraan toisilleen viestivien laitteiden tulee tietää toistensa todelliset IP-osoitteet ja näin ollen WebRTC mahdollistaa yksityisen IP-osoitteen vuotamisen.

Kaiken kaikkiaan selaimesta kerättäviä tietoja on runsaasti, joiden avulla yksittäinen selain pystytään tunnistamaan. EFF (Electric Frontier Foundation) on aloittanut Panopticlick-projektin, jonka avulla käyttäjä voi käydä testaamassa selaimensa jättämää sormenjälkeä. Myös muut sivustot, kuten esimerkiksi Am I Unique? -sivusto, jota rahoittaa mm. DIVERSIFY European -projekti, on kehittänyt oman sormenjälkitestauksen. Menemällä osoitteeseen https://amiunique.org/ voi suorittaa testin, jonka tuloksesta näkee, kuinka tunnistettava sormenjälki on muihin verrattuna (ks. kuva 1).

Are you unique?

Almost! (You can most certainly be tracked.)

41.96 % of observed browsers are **Firefox**, as yours.

0.33 % of observed browsers are **Firefox 63.0**, as yours.

56.55 % of observed browsers run **Windows**, as yours.

21.78 % of observed browsers run **Windows 10**, as yours.

63.15 % of observed browsers have set **"en"**as their primary language, as yours.

20.80 % of observed browsers have **UTC+2** as their timezone, as yours.

But **only** 2 browsers out of the 877362 observed browsers (0.00 %) have exactly the same fingerprint as yours.

My fingerprint

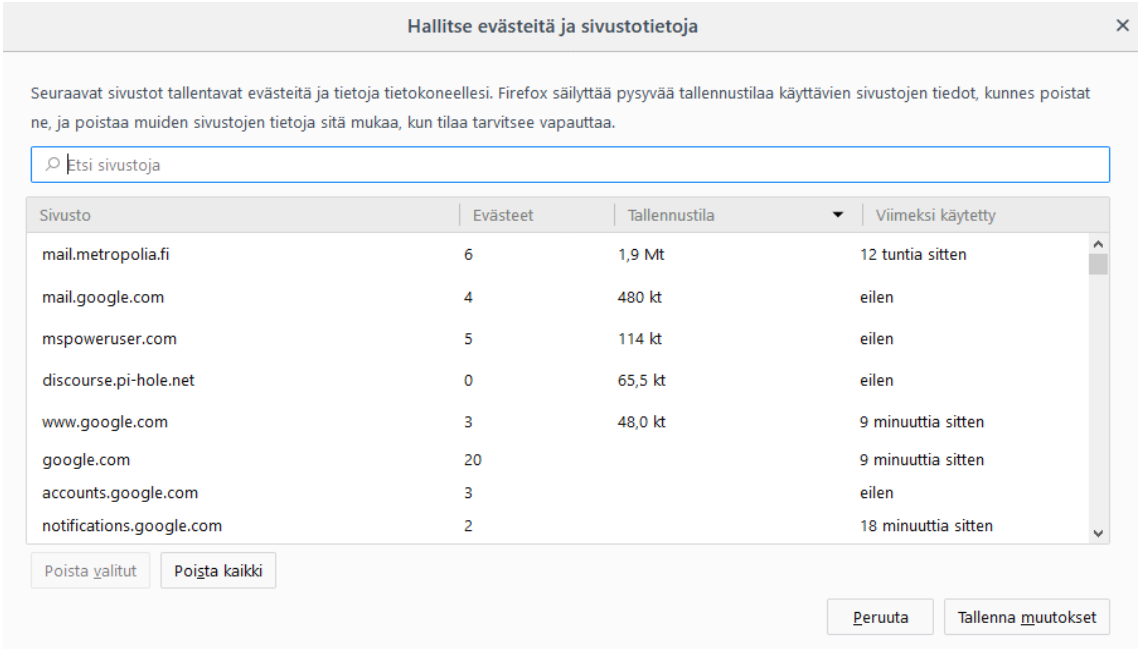
Attribute	Similarity ratio	Value
User agent	0.15%	"Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0"
Accept	54.28%	"text/html,application/xhtml+xml,application/xml;q=0.9;/*;q=0.8"
Content encoding	52.51%	"gzip, deflate, br"
Content language	1.61%	"en-GB,en;q=0.5"
List of plugins	<0.1%	"Plugin 0: Shockwave Flash; Shockwave Flash 30.0 r0; NPSWF64_30_0_0_134.dll. "
Detail of the plugins		
	28.26 %	Shockwave Flash
Platform	39.06%	"Win32"
Cookies enabled	80.29%	"yes"
Do Not Track	32.39%	"yes"
Timezone	20.81%	"-120"
Screen resolution	9.42%	"1366x768x24"
Use of local storage	77.84%	"yes"
Use of session storage	77.84%	"yes"
Canvas	0.55%	Cwm fjordbank glyphs vext quiz, 😃 Cwm fjordbank glyphs vext quiz, 😃
WebGL Vendor		"Google Inc."
WebGL Renderer		"ANGLE (Intel(R) HD Graphics 3000 Direct3D11 vs_4_1 ps_4_1)"
List of fonts	13.19%	"Flash detected but not activated (click-to-play)"
Screen resolution	13.19%	"Flash detected but not activated (click-to-play)"
Language	13.19%	"Flash detected but not activated (click-to-play)"
Platform	13.19%	"Flash detected but not activated (click-to-play)"
Use of AdBlock	33.90%	"yes"

Kuva 1. Am I Unique? -sivuston tulos.

Vaikka suurimman osan seurannasta saakin estettyä rajoittamalla JavaScriptin käyttöä selaimessa, sitä ei voi pitää käytännöllisenä ratkaisuna, koska se rikkoisi suurimman osan sivuistoista ja niiden toiminnoista. Parempana tapana pidetään ns. massaan sulautumista käyttämällä yleisimpiä selaimia kuten Chromea tai Firefoxia käyttämällä selaimen tarjoamia oletusasetuksia kuten englannin kieltä ja käyttämällä yleisimpiä lisäosia. Kuvassa 1 olevia tietoja voidaan muuttaa joko manuaalisesti tai lisäosia käyttämällä, mutta tämä voi mahdollistaa jopa paremman tunnisteen luomisen, koska suurin osa käyttäjistä ei suojaa toimintaansa mitenkään.

3.2 Evästeet

Eväste (cookie) on pieni, yleensä tekstimuotoinen tiedosto, jonka palveluntarjoajan palvelin lähettää selaimelle (ks. kuva 2). Selain tallentaa tiedoston tietokoneelle joko väliaikaisesti tai siihen asti, kunnes se poistetaan. Evästeitä on kahta tyyppiä: istuntokohtainen ja pysyvä. Istuntokohtainen eväste vanhenee, kun käyttäjä lopettaa istunnon eli poistuu palvelusta. Pysyvä eväste säilyy tietokoneella joko ennalta määrätyn ajan tai kunnes käyttäjä poistaa sen. Evästeiden avulla käyttäjä pysyy esimerkiksi kirjautuneena liikkuessaan verkkosivuilla.



Kuva 2. Selaimen tallentamia evästeitä.

Evästeet kehitettiin alun perin parantamaan verkkokaupan toimintaa. Tarkoituksena oli, että ostokset pystyttäisiin yhdistämään asiakkaaseen ja että tämä voitaisiin tunnistaa myöhemmin uudelleen. Evästeitä alettiin kuitenkin nopeasti käyttää seurantaan myös muilla sivustoilla. Näin syntyi kolmannen osapuolen evästeet, jotka seuraavat käyttäjää ympäri internetiä. Esimerkiksi useilta sivuilta löytyvä Facebookin tykkäysnappi on kolmannen osapuolen eväste. [1, s. 47] Useimmissa selaimissa on mahdollista kieltää kolmannen osapuolen evästeet.

Evästeet itsessään ovat anonyymejä, eikä niillä suoraan voida tunnistaa käyttäjää, mutta yritykset kehittävät jatkuvasti uusia ratkaisuja, joilla käyttäjä voidaan tunnistaa yhdistelemällä evästetietoja muiden tietojen kanssa. [1, s. 48.]

Tavallisten evästeiden lisäksi on kehitetty evästeitä, joiden tarkoitus on pysyä tallessa, vaikka käyttäjä yrittäisi poistaa ne. Tällaisia evästeitä kutsutaan nimillä evercookie ja zombiecookie. Ne tallentuvat mahdollisimman moneen eri paikkaan selaimessa, ja niin pitkään, kuin edes yksi eväste on tallella, se luo itsensä uudelleen paikkoihin, joista se on poistettu. [24.]

3.3 Sähköpostin seuranta

Yleisempiä sähköpostipalveluja ovat Googlen Gmail, Microsoftin Outlook.com, Applen iCloud sekä Yahoo Mail. Vaikka näitä kaikkia voidaan pitää suhteellisen turvallisina, niiden yksityisyydensuojassa on puutteita. Kyseisistä palveluista Google, Apple ja Yahoo toteuttavat sähköpostiviestien salauksen TLS-salausprotokollalla tai sen edeltäjällä, SSL-salausprotokollalla. Microsoftin Outlook.com on vuoden 2018 maaliskuussa ottanut käyttöön yksityisyydensuojan kannalta turvallisemman päästä päähän -salauksen (E2EE). E2EE-suojauksessa käyttäjä salaa viestin, ja vastaanottaja purkaa sen, eikä edes sähköpostipalveluntarjoaja pysty näkemään viestin sisältöä. TSL/SSL-salauksessa käyttäjä salaa viestin, joka lähetetään vastaanottajan palveluntarjoajalle. Palveluntarjoaja purkaa viestin, salaa sen uudelleen, ja välittää vastaanottajalle.

Google on skannannut käyttäjiensä sähköposteja aina viime vuoteen asti. Skannausta tehtiin, jotta käyttäjälle pystyttiin näyttämään kohdennettuja mainoksia. Vaikka Google

itse ei enää käy läpi käyttäjien sähköposteja, se antaa kolmansien osapuolien sovelluskehittäjille mahdollisuuden siihen. Tähän toki vaaditaan käyttäjän suostumus, ja Google kertoo vahtivansa sovellusten toimintaa. [25.]

Vuonna 2016 paljastui, että Yahoo oli luovuttanut NSA:lle käyttäjien sähköposteja. Lisäksi Yahoo on kärsinyt useista tietovuodoista vuosien varrella, ja yli miljardin käyttäjän tiedot ovat päätyneet ulkopuolisten tahojen käsiin. [26.]

Sähköposteja seurataan myös pikseliseurannalla (pixel tracking). Se tarkoittaa käyttäjän seurantaa pikselin avulla. Yksinkertaisimmillaan seuranta suoritetaan lisäämällä viestiin 1x1 pikselin kuva (pixel tracker, pixel tag). Pikseli on läpinäkyvä tai samanvärinen kuin tausta, jolla se sijaitsee ja se piilotetaan tarkoituksellisesti käyttäjältä. Kun käyttäjä avaa sähköpostin, pikseli latautuu sen mukana lähettäen pyynnön palvelimelle, jolla se sijaitsee. Pikselin lisääjä voi siten palvelimelta nähdä kuinka monta kertaa pikseli on ladattu. [27.]

Pikseliseurannalla lähettäjä näkee, milloin vastaanottaja on avannut sähköpostin, kuinka monta kertaa se on avattu ja kuinka kauan sitä on luettu sekä onko sähköpostissa mahdollisesti ollutta linkkiä klikattu. Myös palveluntarjoaja, IP-osoite, maantieteellinen sijainti ja käytetty laite käy ilmi. Sähköpostin seurantaa käytetään yleisesti hyväksi verkkomarkkinoinnissa, mutta myös tietojen kalastelijat ja roskapostittajat käyttävät metodia. Mainostajat haluavat varmistaa, että lähetetyt viestit menevät perille ja ne luetaan, mutta väärinkäyttäjät yrittävät etsiä heikkouksia ja kerätä tietoja. Pikseliseurantaa käytetään myös verkkosivujen käytön seurantaan. [27.]

Sähköpostin seurannalta voi suojautua käyttämällä lisäosaa, joka ilmoittaa seurannasta ja estää sen.

3.4 Doksaus

Doksaamisella, doxxing, tarkoitetaan internetissä tapahtuvaa henkilökohtaisten ja yksityisten tietojen etsimistä, keräämistä ja luvatonta jakelemista. Tietoa löytyy yksinkertaisella verkkohaulla, kuten sosiaalisen median sivustoilta, joilla ihmiset jakavat paljon hen-

kilökohtaisia tietoja. Esimerkiksi Facebookin, Twitterin ja LinkedInin kautta voi saada selville puhelinnumeron, työpaikan, sähköpostiosoitteen ja syntymäpäivän. Lisäksi julkaistuista valokuvista voi saada tietoa, missä henkilö liikkuu tai asuu. Keskustelupalstoilla saatetaan jakaa omia kokemuksia ja tarinoita, joista saadaan lisää tietoa. IP-osoitteen perusteella voi saada selville maantieteellisen sijainnin. Yksittäisinä palasina tiedot eivät kerro paljoa, mutta yhdistelemällä tietoja saadaan rakennettua yllättävän tarkka profiili. Doksaamisen tavoitteena yleensä on pahantahtoinen toiminta, kuten kiristäminen, nettikiusaaminen tai omankädenoikeuden harjoittaminen, mutta myös lainvalvojat tai bisnesanalysoijat voivat käyttää hyväkseen doksaamisella saatuja tietoja. [28.]

Doksaamiselta voi suojautua pitämällä huolta, ettei julkaise verkossa henkilökohtaisia tietoja. Myös ajoittainen keskustelupalstoille kirjoitettujen viestien poistaminen suojaa tiedonkeruulta. Saman käyttäjänimen tai sähköpostiosoitteen käyttäminen eri palveluissa on hyvin yleistä, mutta sitä kannattaa välttää.

4 Yksityisyyden suojaaminen

4.1 HTTPS

HTTP (Hypertext Transfer Protocol) on selainten ja WWW-palvelimien käyttämä tiedonsiirtoprotokolla. HTTP-yhteydessä tiedonsiirto tapahtuu kahden keskenään kommunikoivan osapuolen välillä suojaamattomana, jolloin tapahtuvaa tiedonsiirtoa voidaan potentiaalisesti seurata.

HTTPS-protokolla (Hypertext Transfer Protocol Secure) on HTTP-protokollan laajennus, jonka tarkoituksena on suojata tiedonsiirto verkossa. HTTPS-protokollassa tiedot salataan ennen lähettämistä TLS-protokollan (Transport Layer Security) tai sen edeltäjän SSL-protokollan (Secure Sockets Layer) avulla. HTTPS-protokolla suojaa mies välissä - tai välistävetohyökkäykseltä (man-in-the-middle attack). Hyökkäyksessä kahden viestijän väliin tunkeutuu kolmas osapuoli, joka esittää kummallekin viestivälle osapuolelle olevansa toinen viestijä. HTTPS yhteyttä käytettäessä viestivät osapuolet voivat todistaa identiteettinsä kryptografisilla varmenteilla, jolloin kolmas osapuoli ei pysty matkimaan kumpaakaan.

HTTPS-protokollan käyttö on yleistynyt varsinkin NSA-vakoiluskandaalin jälkeen, jolloin paljastui, että NSA oli seurannut useiden HTTP-protokollaa käyttävien sivustojen liikennettä (ks. kuva 3). HTTPS-yhteyttä kannattaakin käyttää aina kun mahdollista. Sen voi tehdä esimerkiksi HTTPS Everywhere -selainlaajennuksella. Se on The Tor Projectin ja EFF:n ilmainen avoimeen lähdekoodiin perustuva laajennus Google Chromelle, Mozilla Firefoxille, Operalle, Bravelle ja Firefoxin Android-versiolle, joka pakottaa HTTPS-yhteyden käytön aina, kun se on mahdollista.

Kuva 3. NSA:n vuodettu dokumentti HTTP-liikenteen seurantaan liittyen. (Lähde: https://www.aclu.org)

4.2 VPN

VPN (Virtual Private Network) on tekniikka, jolla voidaan ulottaa yksityinen verkko toimimaan julkisen verkon yli. VPN kehitettiin alun perin yritysten käyttöön, kun haluttiin, että etäkäyttäjät ja haarakonttorit saisivat luotettavan yhteyden pääkonttorin verkkoon. Nykyään VPN:n käyttö on yleistynyt myös kuluttajien keskuudessa. VPN:n tuoman suojan lisäksi monet käyttävät sitä kiertääkseen maakieltoja internetin eri palveluissa, kuten Netflixissä. VPN:ää käytetään myös kiertämään valtion sensuuria, ja sen käyttö maailmanlaajuisesti on yleisintä Kiinassa, Saudi-Arabiassa, Arabiemiraateissa, Thaimaassa ja Turkissa. Nämä maat myös suoriutuivat huonosti vuoden 2018 internet freedom -indeksissä, joka kertoo internetin vapauden tilasta eri maissa. [29; 30.]

VPN-yhteys toteutetaan tunneloinnilla. On olemassa monia eri tunnelointiprotokollia, joilla VPN-yhteys on mahdollista toteuttaa. Tunnelointiprotokollia käytetään yhdessä salausprotokollien kanssa liikenteen salaamiseksi. Yleisesti näiden kahden protokollan yhdistelmiä voidaan kutsua VPN-protokolliksi:

- PPTP (Point-to-Point Tunneling Protocol) on yksi vanhimmista aktiivisessa käytössä olevista tunnelointiprotokollista. Sen on kehittänyt Microsoft vuonna 1995. Se käyttää 128-, 56- tai 40-bittistä salausta, joka toteutetaan MPPE-salauksella (Microsoft Point-to-Point Encryption).
- L2TP/IPSec on yhdistelmä kahdesta eri protokollasta. L2TP-tunnelointiprotokollaa (Layer 2 Tunneling Protocol) käytetään yhdessä IPSec-salausprotokollan (Internet Protocol Security) kanssa. L2TP kapseloi datan, kun IPSec-protokolla salaa sen.
- IKEv2-protokolla (Internet Key Exchange version 2) on uudempi versio IKE-protokollasta, joka julkaistiin vuonna 2005. L2TP:n tavoin se käyttää IPSec-salausprotokollaa.
- OpenVPN on vuonna 2001 julkaistu avoimen lähdekoodin VPN-protokolla. Sitä pidetään yhtenä maailman turvallisimmista protokollista.
- SSTP (Secure Socket Tunneling) on Microsoftin kehittämä tunnelointiprotokolla, joka julkaistiin Windows Vistassa. SSTP käyttää SSL lähetyksiä IPSecin sijaan, koska SSL tukee verkkovierailuja. [31.]

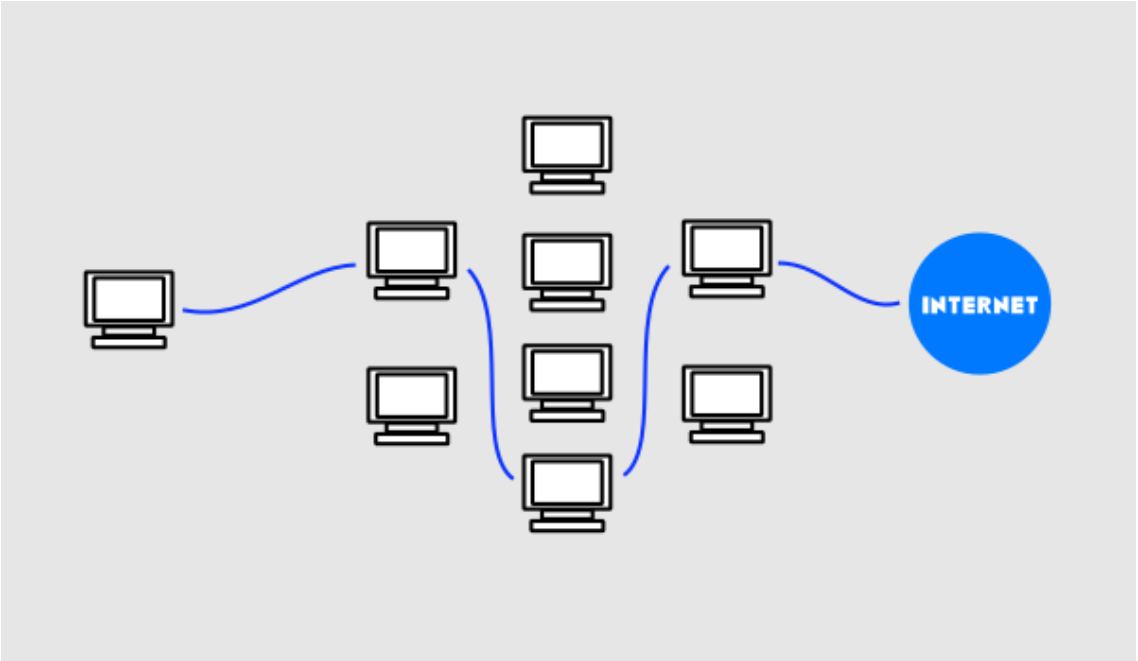
VPN-palvelua valittaessa on otettava huomioon, että palveluntarjoajalla on tekninen mahdollisuus nähdä ja tallentaa kaikki liikenne, joka tapahtuu sen palvelimien kautta. Kannattaa siis valita VPN-palveluntarjoaja, johon todella luottaa. Palveluntarjoajan käyttöehdoista pitäisi löytyä tietoa siitä, miten käyttäjien tietoja käsitellään ja kirjataanko käyttäjän tietoliikennettä tai muuta toimintaa. Hintavertailua kannattaa tehdä, mutta pitää myös mielessä, että yleensä ilmainen palvelu tarkoittaa tuoton hankkimista jostain muualta, yleensä myymällä käyttäjien tietoja eteenpäin. Nopeus on myös yksi valintakriteereistä, ja joskus palveluntarjoajat esittävät sivuillaan saavutettuja nopeuksia. Todellisen kuvan palvelun nopeudesta saa kuitenkin vain kokeilemalla, joten kannattaa valita palveluntarjoaja, joka tarjoaa esimerkiksi kuukauden ilmaista kokeilujaksoa.

Useat VPN-palvelut vuotavat tietoa käyttäjästä. Erään tutkimuksen perusteella jopa 84 % VPN-palveluista vuotaa käyttäjän oman IP-osoitteen. Lisäksi ns. ”kill switch” -toiminto puuttuu osasta palveluita. Kill switch varmistaa, että jos yhteys VPN-palvelimeen katkeaa jostain syystä, myös internetliikenne katkeaa, kunnes yhteys palvelimeen on jälleen saatu. [32.]

4.3 Tor

Tor (The Onion Router) on avoimeen lähdekoodiin perustuva ohjelmisto, joka mahdollistaa käyttäjän verkkoliikenteen anonymisoinnin. Sen kehittivät Yhdysvaltain laivaston tutkimuslaitoksen työntekijät Paul Syverson, Michael Reed ja David Goldschlag 1990-luvun puolivälissä, ja sen alkuperäinen tarkoitus oli suojata Yhdysvaltojen tiedusteluyhteyksiä verkossa. Nykyään sitä käyttävät eri maiden valvontaviranomaisten ja armeijan lisäksi myös tavalliset ihmiset, toimittajat sekä aktivistit useisiin eri tarkoituksiin. Tavalliset ihmiset käyttävät sitä esimerkiksi kiertääkseen palveluntarjoajan asettamia estoja, kun taas toimittajat keskustelevat sen avulla ilmiantajien kanssa.

Tor-ohjelman toiminta perustuu tekniikkaan nimeltä sipulireititys, jolla tarkoitetaan nimensä mukaisesti kerroksellista salausta. Sipulireititys-tekniikalla salataan käyttäjän lähettämä viesti, jonka lisäksi sille luodaan salattu reitti vähintään kolmen eri solmun läpi ennen sen päätymistä internetiin viimeisen solmun kautta (ks. kuva 4). Näitä kutsutaan yleisesti nimillä sisääntulosolmu (entry node, guard), keskimmäinen solmu (middle node) ja ulostulosolmu (exit node). Salattu reitti on ns. kerrostettu tarkoittaen, että jokaisessa salauskerroksessa on vain tieto edellisestä solmusta sekä seuraavasta, johon tieto lähetetään. Jokaisella solmulla on yksi osa koko salauspaketin avaimista, jolloin jokainen solmu pystyy avaamaan yhden salauskerroksen. Solmun viimeisellä osalla (exit node) on avain alkuperäisen viestin avaamiseen, joka sen jälkeen lähetetään normaalisti eteenpäin lopulliseen päämääräänsä. [33.]



Kuva 4. Tor-verkon toiminta.

Sipulireitityksen tarkoituksena on suojata viestin lähettäjän alkuperä, sillä jokaisella välityssolmulla on tietoa vain edellisen ja seuraavan solmun osoitteesta pois lukien sisääntulo- (entry node) ja ulostulosolmut. Ensimmäisen solmu tietää lähetetyn viestin alkuperän, mutta ei itse viestiä eikä lopullista päämäärää. Viimeinen solmu puolestaan tietää viestin sisällön, mutta ei alkuperää. Tämän lisäksi Tor vaihtaa 10 minuutin välein yhteyden reittiä, jotta saman reitin solmuja seuraava ei pysty kuuntelemaan liikennettä pitkään.

Tor-verkon käyttämässä tekniikassa huonona puolena on sen hitaus, eikä sitä olekaan tarkoitettu videoiden katsomiseen tai ohjelmistojen lataamiseen. Tällä hetkellä Tor-verkossa on mahdollista siirtää keskimäärin 1 MB dataa kolmessa sekunnissa, jolloin yleiseksi siirtonopeudeksi voidaan laskea 2,8 Mbps.

Tor-liikennettä ohjataan yli kuudesta tuhannesta solmusta koostuvan maailmanlaajuisen vapaaehtoisesti ylläpidetyn verkoston kautta. Kuka tahansa pystyy käyttämään Tor-verkkoa sekä ylläpitämään omaa solmua Tor-verkossa. Tässä piilee Tor-verkon vahvuus ja samalla sen heikkous. Koska kuka tahansa, joka pystyy ylläpitämään omaa solmua, voi tallentaa tietoja sen läpi menevästä liikenteestä. Vaikka yhdestä solmusta kerättävä tieto

yksinään ei ole hirveän hyödyllistä, monet maat omistavat hyvin todennäköisesti satoja, ellei tuhansia, solmuja ja seuraavat liikennettä niiden kautta.

Tor-käyttäjän identiteetti on mahdollista selvittää ns. päästä-päähän-hyökkäyksen avulla (End-to-End Confirmation Attack). Tässä hyökkäyksessä ei ole tarkoitus purkaa salattua liikennettä, vaan etsiä liikenteestä toistuvia kuvioita kuten lähetettyjen pakettien kokoja ja niiden lähetysaikoja. Esimerkiksi voidaan tallentaa verkkosivun avaushetkellä tapahtuva liikenne. Tällöin saadaan selville, kuinka monta pakettia lähetettiin molempiin suuntiin sekä niiden koot ja aikaleimat. Näin luodaan verkkosivulle sormenjälki, jota voidaan verrata salattuun liikenteeseen Tor-verkon läpi. Tämä kuitenkin vaatii vähintään sisääntulosolmun kuuntelua, jolloin käyttäjän liikennettä voidaan verrata tarkkailun alaisen sivuston sormenjälkeen.

Tor-verkkoa on mahdollista käyttää monella eri tavalla, mutta on suositeltavaa käyttää Tor-projektin omia virallisia ohjelmia. Näihin lukeutuu Tor-selain, joka voidaan asentaa Windows-, Linux- ja MacOS-käyttöjärjestelmille. Se on muokattu versio Firefoxin selaimen ESR-versiosta (Extended Support Release). Älypuhelimille löytyvät myös omat selaimensa, Orfox (Android) ja Onion Browser (iOS). Android-käyttöjärjestelmille on myös mahdollista asentaa Tor-projektin luoma VPN-palvelu Orbot. Tor-projektin kotisivuilta on ladattavissa myös Tails-käyttöjärjestelmä, joka asennetaan USB-tikulle tai DVD-levylle, jolloin käyttöjärjestelmää ei asenneta itse laitteelle ja sen käyttö onnistuu suoraan tikulta tai levyltä. On myös mahdollista konfiguroida reititin käyttämään Tor-verkkoa, mutta tämä ei ole suositeltua, koska reititin reitittää kaiken liikenteen silloin saman Tor-yhteyden kautta. [34.]

4.4 Ohjelmistot

Yleisimmin käytetyt ohjelmistot saattavat olla uhka yksityisyydelle mm. niiden keräämien telemetriatietojen takia ja usein kannattaakin tutkia eri vaihtoehtoja. Esimerkiksi sähköpostille, selaimelle ja hakukoneelle on tarjolla turvallisempia vaihtoehtoja.

Maailman käytetyin hakukone on Google n. 70 %:n markkinaosuudellaan. Kuten monet muutkin suurimmat hakukoneet se tallentaa oletuksena käyttäjien hakutiedot. Yksityisyyttä kunnioittavia vaihtoehtoja on kuitenkin kehitetty, esimerkiksi DuckDuckGo- ja Startpage-hakukoneet.

DuckDuckGo-hakukone ei jäljitä käyttäjää. Se estää mainosten seurannan, pitää hakuhistorian yksityisenä ja antaa käyttäjälle mahdollisuuden hallita yksityistä dataa. Mainosten seurannan esto tarkoittaa, ettei käyttäjälle näytetä kohdennettuja mainoksia. Hakuhistoriaa ei tallenneta, joten sitä ei myydä eteenpäin. Mitään henkilökohtaisia tietoja ei tallenneta eikä jaeta eteenpäin. Startpage-hakukoneessa on toimintoina proxy-palvelun käyttö, HTTPS-tuki ja URL-generaattori, joka eliminoi tarpeen evästeiden käyttöön. Se ei tallenna mitään tietoja käyttäjästä.

Yksityisyydensuojaa kunnioittavista sähköpostipalveluista voidaan mainita esimerkiksi ProtonMail, josta löytyy tuki E2EE-salaukselle. Sitä on mahdollista käyttää täysin anonyymisti, eikä käyttäjien toimintaa seurata. ProtonMaililla voi lähettää viestejä, jotka tuhoutuvat tietyn ajan kuluttua itsestään. Sen palvelimet sijaitsevat Sveitsissä, joten niihin ei sovelleta Yhdysvaltojen tai Euroopan unionin lakeja. [35.]

Monet internetin palvelut vaativat nykyään jonkinasteisen rekisteröitymisen, ja usein siihen riittää vain sähköposti. Sähköpostiosoitteen jakaminen kuitenkin mahdollistaa sen päätymisen markkinointitarkoituksiin ja joskus kannattaakin turvautua väliaikaisen sähköpostin käyttöön esimerkiksi tilanteessa, jossa palvelua käytetään vain kerran. Väliaikainen sähköpostiosoite on kertakäyttöinen, ja se tuhoutuu tietyn ajan kuluttua. Tällainen sähköpostipalvelu on esimerkiksi 10minutemail.

5 Kotiverkon suojauksen suunnittelu

Osana insinöörityötä haluttiin toteuttaa kotiverkon suoja seurantaa vastaan. Projektissa käytettäväksi laitteeksi valittiin yhden piirilevyn tietokone Raspberry Pi sen kohtuullisten aloitus- ja käyttökustannuksien vuoksi. Samassa hintaluokassa on tarjolla muitakin yhden piirilevyn tietokoneita, esimerkiksi Asus Tinker Board, Banana Pi ja Pine, joista osa on jopa tehokkaampia vaihtoehtoja kuin Raspberry Pi. Raspberry Pi:n etuna on kuitenkin suuri käyttäjä- ja kehittäjäyhteisö, jonka seurauksena tuki eri sovellusten suunnitteluun ja rakentamiseen on paremmin löydettävissä.

Projektissa haluttiin suojata kaikki verkkoon liitetyt laitteet seurannalta ja telemetriatietojen keräämiseltä. Yleinen ratkaisu seurannan estämiseksi on asentaa selaimelle seurannan- ja mainonnanestolaajennuksia, kuten uBlock Origin, Adblock Plus ja Ghostery. Laajennukset toimivat kuitenkin selainkohtaisesti, joten ne on asennettava jokaiselle laitteelle ja selaimelle erikseen. Laajennusten käytön rajoitteena koko kotiverkon suojaamisen kannalta on se, ettei kaikilla verkkoon liitetyillä laitteilla ole selainta, ja vaikka sellainen olisi, siihen ei pysty asentamaan lisäosia, esimerkkinä älytelevisio tai pelikonsoli.

Projektissa pohdittiin eri toteutustapoja kotiverkon suojaamiseksi, kuten oman välitys- tai DNS-palvelimen luonti. Lopulta suojaus päätettiin toteuttaa oman DNS-palvelimen luomisella, sillä se on kevyempi ratkaisu verrattuna välityspalvelimen käyttöön. Projektissa vertailtiin vastakkain kahta eri DNS-tason seurannan- ja mainonnanesto-ohjelmaa: Pi-holea ja AdGuard Homea. Molemmat ratkaisut olivat hyvin lähellä toisinaan toimivuuden ja toteutuksen kannalta. DNS-palvelimen luonti päätettiin kuitenkin toteuttaa Pi-hole-ohjelmalla, koska siitä oli jo julkaistu monta virallista versiota, kun taas AdGuard Home on vielä beta-vaiheessa.

Pi-holen toimintaa päätettiin laajentaa myös kotiverkon ulkopuolelle. Tämä toteutettiin oman VPN-palvelimen avulla, joka konfiguroitiin toimimaan yhdessä Pi-holen kanssa. VPN-palvelinratkaisu toteutettiin OpenVPN:llä sen turvallisuuden ja luotettavuuden takia.

6 Raspberry Pi

Raspberry Pi on hieman luottokorttia isompi yhden piirilevyn pienoistietokone, jonka on kehittänyt brittiläinen Raspberry Pi Foundation. Se kehitettiin ensisijaisesti opetus- ja harrastuskäyttöön. Pienen kokonsa ja hintansa ansiosta Raspberry Pi keräsi suuren määrän kiinnostusta eri puolilla maailmaa, kun se julkaistiin vuonna 2012. Raspberry Pi:stä on julkaistu monta eri tuotemallia erikokoisille piirilevyille (Model A, Model B, Compute module, Zero). Ensimmäinen Raspberry Pi julkaistiin vuonna 2012 ja siitä on kirjoitushetkellä olemassa yhteensä 14 eri versiota.

6.1 Arkkitehtuuri ja tekniset tiedot

Raspberry Pi perustuu ARM-arkkitehtuuriin ja käyttöjärjestelmänä ensimmäisissä versioissa toimi lähtökohtaisesti vain Linux-pohjainen Raspberry Pi:lle räätälöity Raspbian-käyttöjärjestelmä. Nykyään Raspberry Pi tukee myös monia muitakin Linux-pohjaisia käyttöjärjestelmiä sekä Microsoftin vuonna 2018 julkaisemaa Windows 10 IoT Corea.

Työssä käytetään paranneltua kolmannen sukupolven Raspberry Pi Model B:tä, nimeltään Raspberry Pi 3 Model B+, joka julkaistiin maaliskuussa 2018. Se sisältää 1,4 GHz:n taajuudella toimivan Cortex-A53-neliydinprosessorin, 1 Gt keskusmuistia, HDMI-portin, Gigabit Ethernetin, 4 USB-porttia, microSD-muistikorttipaikan sekä 802.11ac-standardin mukaisen 2,4 GHz:n ja 5 GHz:n WLAN-yhteyden. [36]

Paranneltu Raspberry Pi 3 Model B+ eroaa edellisestä versiosta nopeammalla prosessorilla, gigabitin verkkoliitännällä ja nopeammalla WLAN-yhteydellä. Lisäksi siinä on uudempi järjestelmäpiiri, joka korjaa edellistä mallia vaivanneet ylikuumenemisongelmat sekä mahdollisuus PoE-käyttöön (Power over Ethernet).

6.2 Raspberry Pi:n asennus

Raspberry Pi:n käyttöönotto on hyvin suoraviivaista ja siihen löytyy yksityiskohtaiset ohjeet Raspberry Pi Foundationin kotisivuilta https://www.raspberrypi.org/documentation/installation/. Valmiita asennussarjoja on myynnissä, johon kuuluu itse Raspberry Pi,

kotelo, virtalähde sekä muistikortti, josta löytyy valmiiksi NOOBS-asennusohjelma (New Out Of the Box Software), joka on helppokäyttöinen käyttöjärjestelmän asennusohjelma, jota suositellaan aloittelijoille.

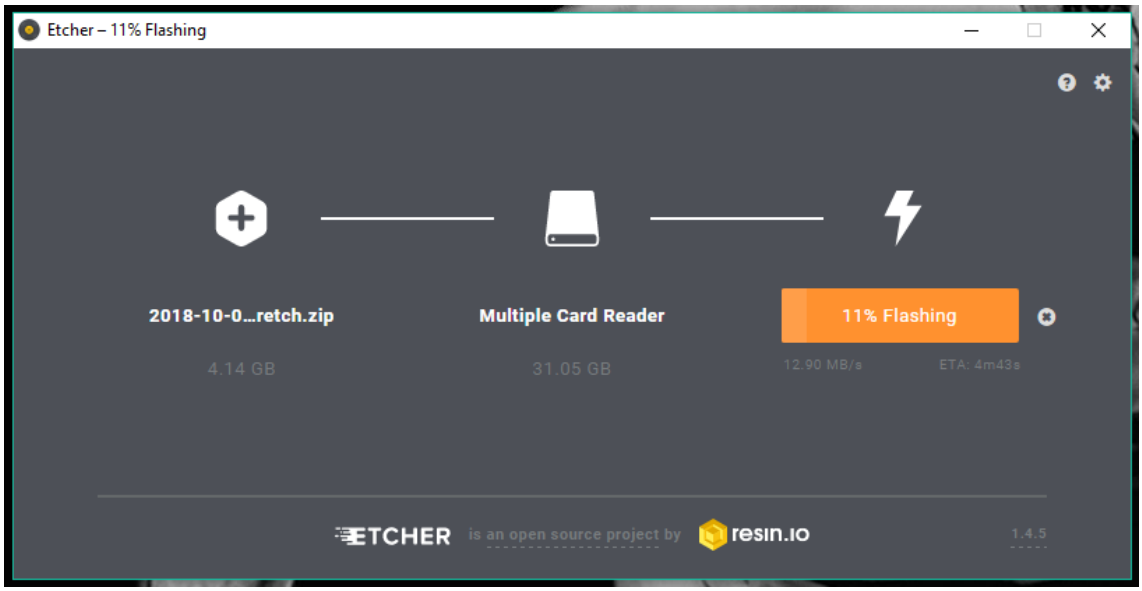
Raspberry Pi:n käyttöönottoon tarvitaan:

- Raspberry Pi
- virtalähde
- microSD-muistikortti (suositus vähintään 8 GB)
- näyttö
- HDMI-kaapeli
- hiiri ja näppäimistö

Normaaliin asennussarjaan kuuluvat osat ostettiin työtä varten erikseen, koska se tuli halvemmaksi. Vaikka NOOBS-asennusohjelmalla varustettuja MicroSD-muistikortteja on mahdollista ostaa erikseen, on pääsääntöisesti halvempaa ostaa normaali MicroSD-muistikortti, johon asennetaan haluttu käyttöjärjestelmä. Tämä vaatii kuitenkin tietokoneen, muistikortinlukijan sekä useimmiten muistikorttiadapterin.

Käyttöjärjestelmäksi valittiin Raspberry Pi Foundationin kehittämä Raspbian Stretch with Desktop, joka perustuu Debian-käyttöjärjestelmään. Sen levykuva on ladattavissa osoitteesta https://www.raspberrypi.org/downloads/raspbian/.

Asennukseen tarvitaan muistikortin kirjoitustyökalu. Raspberry Pi:n kotisivuilla suositellaan käyttämään Etcheriä, joka on graafisen käyttöliittymän ansiosta todella helppokäyttöinen (ks. kuva 5). Se tunnistaa automaattisesti tietokoneeseen liitetyn muistikortin, jonka jälkeen valitaan käyttöjärjestelmän levykuva kansiosta, jonne se on tallennettu. Etcher tukee myös levykuvan kirjoittamista suoraan pakatusta tiedostosta ilman, että sitä tarvitsee purkaa.



Kuva 5. Etcher-kirjoitustyökalu toiminnassa.

Levykuvan kirjoituksen jälkeen muistikortti on valmis asetettavaksi Raspberry Pi:hin, ja asennus alkaa automaattisesti ensimmäisen käynnistyksen yhteydessä. Tämän jälkeen Raspberry Pi on valmis käytettäväksi.

6.3 Tarvittavat esiasetukset

Raspberry Pi:n ensikäynnistyksen yhteydessä päivitetään Raspberry Pi -komennoilla:

sudo apt-get update
sudo apt-get dist-upgrade

Kaikissa Raspberry Pi-laitteissa, joissa on asennettuna Raspbian, käyttäjätunnus ja salasana, on oletuksena sama: pi ja raspberry. Onkin tärkeää vaihtaa vähintään oletussalasana heti Pi:n käyttöönotossa. Tämä voidaan toteuttaa raspi-config-käyttöliittymästä. Pelkän salasanan vaihtamisen sijaan suositellaan uuden käyttäjän tekemistä ja oletuskäyttäjä pi:n poistamista. Oletuskäyttäjätunnuksen käyttämistä kannatta välttää, sillä silloin potentiaalisen hyökkääjän tarvitsee enää selvittää salasana.

Uuden käyttäjän luominen sudo-käyttöoikeuksilla sekä oletuskäyttäjän poistaminen voidaan toteuttaa seuraavilla komennoilla:

sudo adduser [käyttäjänimi]
sudo adduser [käyttäjänimi] sudo
sudo deluser pi

Raspberry Pi suorittaa oletuksena HDMI-laiteskannausta tietyin väliajoin ja katkaisee virran HDMI-portille, jos se ei havaitse näyttöä. Jos laitteelle täytyy myöhemmin tehdä konfiguraatioita, on suositeltavaa pakottaa Raspberry Pi käyttämään HDMI-porttia jatkuvasti. Tämä toteutetaan muuttamalla käynnistystiedoston asetuksia:

sudo nano /boot/config.txt
----
hdmi_force_hotplug=1
hdmi_drive=2
----

7 Pi-hole

Pi-hole on ohjelma, jolla saadaan luotua verkkotason suoja mainontaa ja seurantaa vastaan. Se toimii ns. DNS-kyselyiden valvojana, joka päättää, mitä verkkotunnuksia verkosta haetaan.

Tietokoneet ja muut verkon laitteet tunnistavat ja löytävät toisensa IP-osoitteen perusteella. Ihmiselle olisi hyvin vaikeaa tai jopa mahdotonta muistaa kaikki tarvittavat osoitteet numeerisessa muodossa. DNS eli Domain Name System on internetin nimipalvelujärjestelmä, joka muuntaa IP-osoitteet verkkotunnuksiksi ja pitää kirjaa niistä. Tämä tarkoittaa selaimeen kirjoitetun osoitteen, esimerkiksi google.com, muuntamista sen IP-osoitteeksi, 64.233.162.147. Yksinkertaisimmillaan DNS:ää voikin ajatella puhelinluettelona verkkotunnuksille.

Pi-hole on avoimeen lähdekoodiin perustuva verkkotason mainonnan- ja seurannanesto-ohjelma, jonka kehitys alkoi vuonna 2014. Se on asennettavissa useimmille Debian-pohjaisille jakeluille, ja virallinen tuki on kirjoitushetkellä Raspbianin Jessielle ja Stretchille, Ubuntulle, Debianille, Fedoralle ja Centosille. [37.]

Vaikka Pi-hole on käyttötarkoitukseltaan samanlainen kuin selainten mainonnanestolaajennukset, on sen toimintatapa varsin erilainen. Pi-hole vertaa verkossa olevien laitteiden DNS-kyselyiden verkkotunnuksia omiin listoihinsa, jonka jälkeen se päättää, päästetäänkö kysely läpi vai ei. Jos DNS-kyselyn verkkotunnus löytyy estolistalta, Pi-hole ohjaa kyselyn itselleen ja palauttaa 404-virheilmoituksen laitteelle. Tällä tavalla estetään esimerkiksi mainoskuvan latautumista kotiverkossa, joka puolestaan nopeuttaa verkon toimintaa. [38.]

Toisin kuin selaimiin asennettavat mainonnanestolaajennukset, kuten uBlock Origin ja Adblock, Pi-hole tarkkailee koko verkon toimintaa. Sen avulla pystyy estämään seurantaa ja mainontaa esimerkiksi verkkoon liitetyn älypuhelimen sovelluksista. Tällä tavalla se myös suojaa verkkoon liitettyjä vanhempia laitteita, joihin ei tehdä enää tietoturvapäivityksiä. Pi-holen vahvuus on myös sen heikkous, koska kyseessä on DNS-palvelu, se ei pysty estämään ns. upotettuja mainoksia. Tämä tarkoittaa mainoksia, joita verkkosi-

vusto tarjoaa omasta osoitteestaan. Se ei myöskään pysty minkäänlaiseen sisällön suodattamiseen, toisin kuin selaimessa toimivat mainonnanestolaajennukset. Pi-hole onkin ensisijaisesti tarkoitettu käytettäväksi selainlaajennusten rinnalla lisäsuojana.

7.1 Pi-Holen asennus ja konfigurointi

Ennen Pi-Holen asennusta annetaan Raspberry Pi:lle staattinen IP-osoite, jotta DNS-kyselyt saadaan ohjattua luotettavasti Pi-holen läpi. Tässä projektissa IP-osoitteen määritys tehtiin suoraan reitittimen asetuksista. Raspberry Pi:lle voi määrittää staattisen IP-osoitteen myös laitteen omista asetuksista. Ensin ajetaan ifconfig-komento, jolla saadaan selville verkkokortin nimi:

ifconfig

Tämän jälkeen asetetaan verkkokortille staattinen IP-osoite dhcpcd.conf-tiedostosta avaamalla tekstitiedosto Nano-tekstieditorilla:

sudo nano /etc/dhcpcd.conf

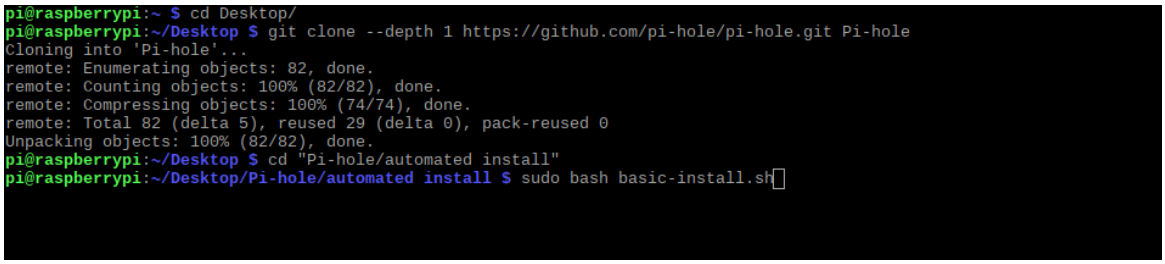
Tiedostoon muokataan alla olevan esimerkin mukaiset arvot:

```
-----------------------------------------------------------
interface [verkkokortin nimi]
static ip_address=192.168.0.2/24
static routers=192.168.0.1
static domain_name_servers=192.168.0.1
-----------------------------------------------------------
```

Asennus aloitetaan lataamalla Pi-Holen repository (tiedostovarasto) Raspberry Pi:lle, jonka jälkeen navigoidaan ladattuun hakemistoon ja suoritetaan asennusskripti (ks. kuva 6).

```
git clone --depth 1 https://github.com/pi-hole/pi-hole.git Pi-hole
cd "Pi-hole/automated install/"
```

sudo bash basic-install.sh



Kuva 6. Pi-holen asennus

Asennusskripti suorittaa siinä olevat komennot, joilla tarkistetaan käytössä oleva käyttöjärjestelmä ja mahdolliset ohjelmariippuvuudet. Tämän jälkeen Pi-Holen asennusohjelma käynnistyy. Asennusohjelmassa määritetään seuraavat toiminta-asetukset:

- DNS-palvelun tarjoaja
- käytettävät estolistat
- estettävät protokollat: IPv4 ja IPv6
- staattisen IP-osoitteen valinta
- käyttöliittymän asennus
- HTTP-palvelinohjelman asennus
- lokitiedostojen tallennus.

Kun Pi-holen asennus on valmis, määritetään reitittimen asetuksista Raspberry Pi toimimaan kotiverkon DNS-palvelun välittäjänä. Toiminnan voi testata menemällä verkkoselaimella Raspberry Pi:lle määritettyyn IP-osoitteeseen ja lisäämällä osoitteen loppuun /admin/. Pi-hole antaa asennuksen yhteydessä käyttäjälle salasanan, jolla kirjaudutaan hallintasivulle. Käyttöliittymään pääsee kaikilta verkossa olevilta laitteilta ja kirjautumatta voi nähdä yleiskatsauksen verkkoliikenteestä.

7.2 Pi-holen käyttöliittymä

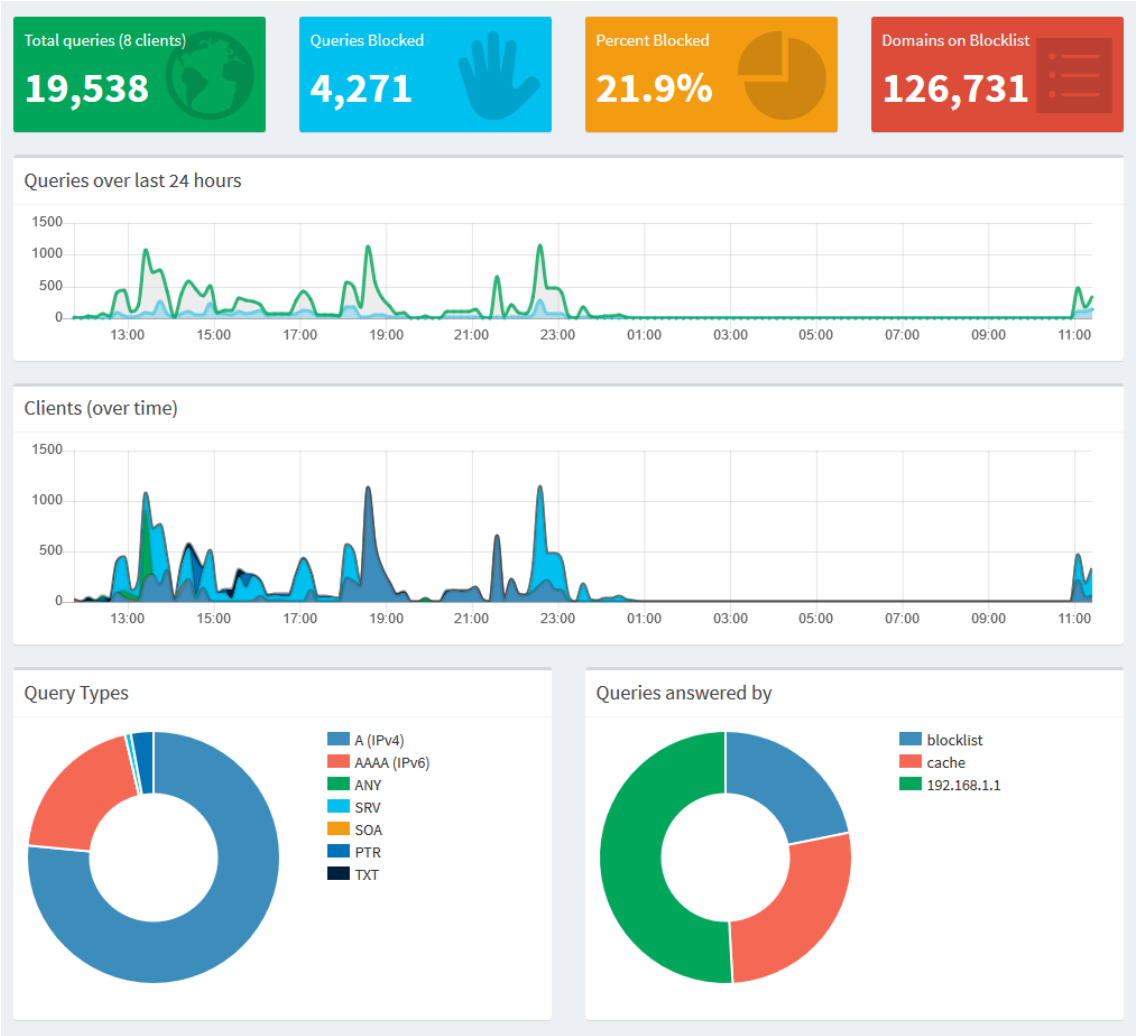
Navigointi Pi-holen käyttöliittymässä tapahtuu vasemmalla sijaitsevan palkin kautta, josta löytyy raportointinäkymän lisäksi:

- Query Log, eli kyselyloki, josta näkee kaikkien kyselyiden tiedot yksityiskohtaisesti tietyn ajanjakson aikana.
- Long Term Data, eli pitkäaikaistiedot esitettyinä joko kaavioina, kyselylokina tai listoina.
- Whitelist, jolla voidaan luoda poikkeuksia estolistoille.
- Blacklist, johon voidaan lisätä estettäviä osoitteita.
- Disable, josta palvelu voidaan kytkeä pois päältä joko pysyvästi tai ennalta määrätyksi ajaksi.
- Tools, eli työkalut, joilla määritetään Pi-holen toimintaa.
- Settings, eli asetukset, josta pääsee luonnollisesti säätämään asetuksia.
- Logout eli uloskirjaus, josta Pi-holen käyttöliittymästä kirjaudutaan ulos turvallisesti.
- Donate, josta ohjataan sivulle, jossa voi tukea Pi-holen toimintaa.
- Help, josta löytyy ohjeita Pi-holen käyttöliittymän eri osioista.

Sivupalkissa on myös Status-alue, joka kertoo, onko Pi-hole aktiivinen, käynnistymässä vai kytketty pois päältä. Lisäksi se kertoo prosessorin lämpötilan ja muistin käyttöasteen.

7.2.1 Raportointinäkymä (Dashboard)

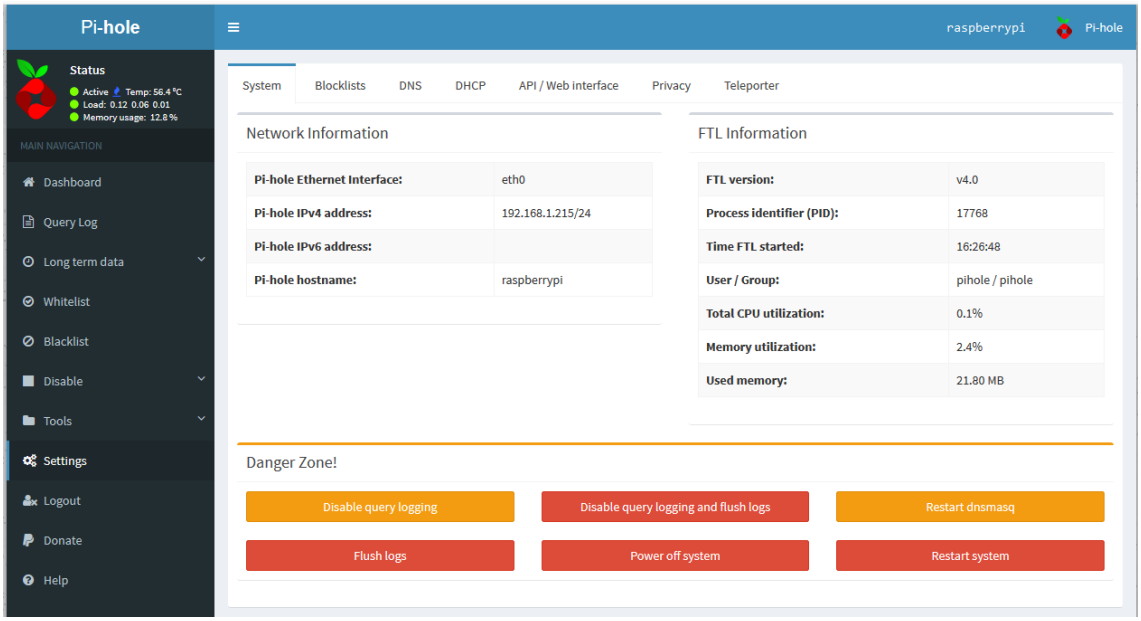
Pi-holen pääsivulta eli raportointinäkymästä näkee erilaisia datakaavioita Pi-holen kautta kulkevasta verkkoliikenteestä. Siitä näkee DNS-kyselyiden kokonaismäärän, estettyjen kyselyiden kokonaismäärän ja osuuden prosentteina sekä estettyjen verkkotunnusten määrän. Lisäksi raportointinäkymästä näkee DNS-kyselyiden määrän viimeisen 24 tunnin ajalta. Raportointinäkymästä löytyy myös kaaviot kyselyiden tyypeistä, joita ovat esimerkiksi A (IPv4-osoitteet), AAAA (IPv6-osoitteet) (ks. kuva 7). Lisäksi löytyvät listat useimmiten sallituista ja estetyistä verkkotunnuksista sekä laitteista.



Kuva 7. Pi-holen raportointinäkymä.

7.2.2 Asetukset (Settings)

Pi-holen asetuksista löytyvät mm. yleiset tiedot laitteesta, jolle se on asennettu, mahdollisuus lisätä tai poistaa estolistoja, DNS- ja DHCP-asetukset sekä mahdollisuus muokata käyttöliittymän näkymää (ks. kuva 8).



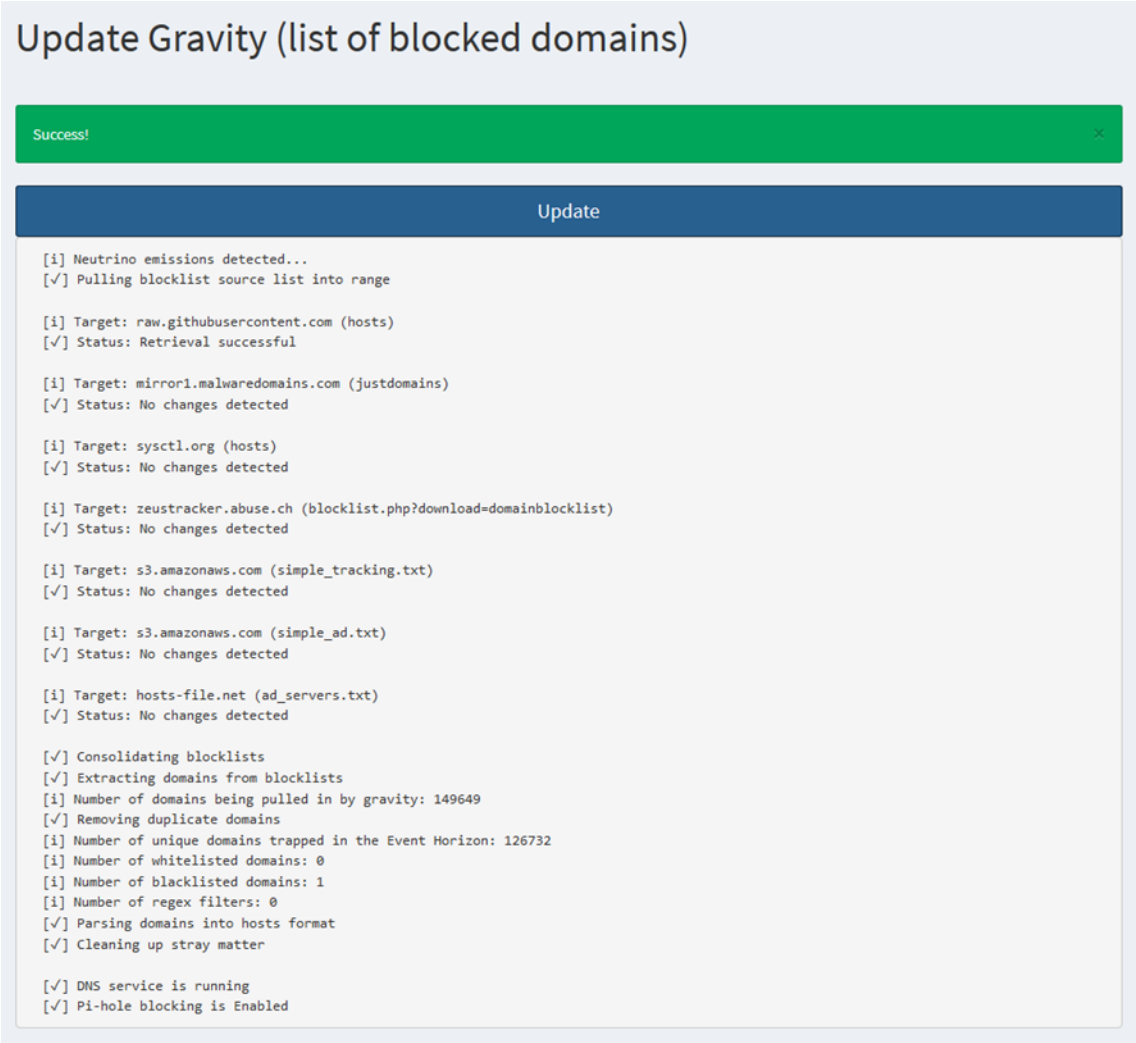
Kuva 8. Pi-holen asetukset

Blocklist-välilehdeltä näkyvät käytössä olevat verkkotunnusten estolistat. Asennusvaiheessa valitut oletuslistat näkyvät täällä. Listoja ylläpidetään vapaaehtoisvoimin ja niitä voi itse lisätä suoraan verkosta, jolloin niiden päivittäminen tapahtuu automaattisesti. Esimerkiksi sivustolta https://tspprs.com/ on ladattavissa estolistoja eri kategorioiden perusteella. Näihin kuuluvat mm. mainonta ja seuranta, telemetria ja haittaohjelmat.

DNS-välilehdeltä on mahdollista määrittää DNS-palvelutarjoaja. Vaihtoehtoina on Google, OpenDNS, Level3, Norton, Comodo, DNS.WATCH, Quad9 ja Cloudflare. On myös mahdollista lisätä itse valittu DNS-palveluntarjoaja. Työssä päätettiin käyttää oman palveluntarjoajan DNS-palvelua.

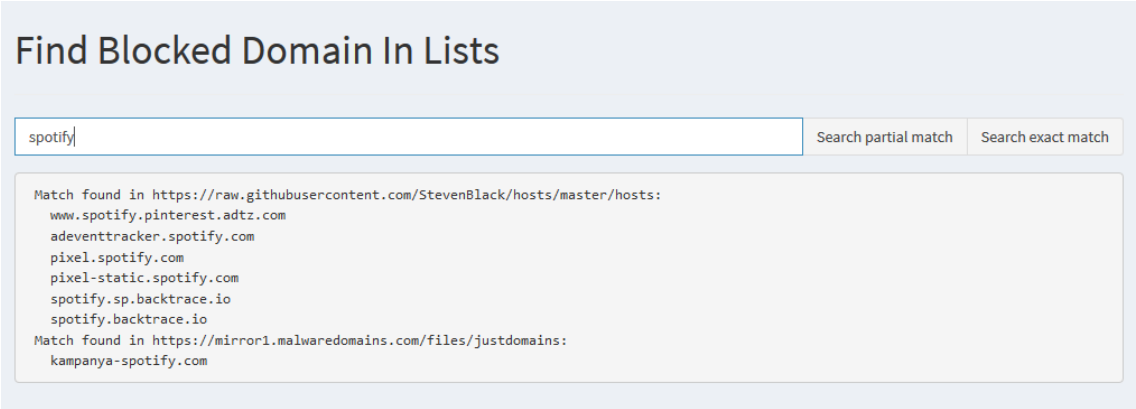
7.2.3 Työkalut (Tools)

Työkaluista löytyy Update Gravity -välilehti, josta pystyy päivittämään Pi-holen estolistat manuaalisesti. Oletuksena estolistat päivitetään kerran viikossa. Päivitys suoritetaan cron-ajastuspalvelulla ja sitä voi muokata /etc/cron.d/pihole-tiedostosta muokkaamalla pihole updateGravity -riviä. Päivityksen jälkeen näkyviin tulee loki, josta näkee yksityiskohtaiset tiedot päivityksestä (ks. kuva 9).



Kuva 9. Pi-holen Update Gravity -päivitysikkuna

Query Lists -välilehdeltä voi etsiä jotain tiettyä verkkotunnusta ja selvittää, millä kaikilla listoilla se esiintyy. Pi-hole ei vahdi, mitä kolmannen osapuolen julkaisijat laittavat esto-listoilleen, ja joskus listoilla voi olla sellaisia verkkotunnuksia, joita ei haluta estää. Jos huomataan, että jokin sivusto ei toimi, voi Query List -hausta katsoa, löytyykö verkkotunnus joltain listalta ja sallia se (ks. kuva 10).



Kuva 10. Pi-holen Query Lists -hakutyökalu

Lisäksi työkaluista löytyy audit log -välilehti, josta näkyvät kaikki verkkotunnukset, jotka ovat Pi-holen lokitiedostossa. Ne voidaan ns. auditoida, jolloin ne lisätään /etc/pihole/auditlog.list-tiedostoon, eivätkä ne enää tulevaisuudessa näy välilehdellä. Näin helpotetaan verkkotunnusten läpikäymistä.

Tail pihole.log -välilehti näyttää reaaliajassa lokitiedostoon tallennettavaa raakadataa kyselyistä ja Tail pihole-FTL.log -välilehdeltä näkee Pi-holen FTL-moottorin (Faster Than Lightning) lokitiedostoon kirjattavaa dataa.

Generate debug log -välilehdeltä käynnistetään prosessi, joka kerää tietoa Pi-holesta ja lopulta luo käyttäjälle selostuksen diagnostiikasta.

8 OpenVPN

OpenVPN on avoimeen lähdekoodiin perustuva SSL VPN -ohjelmisto. Se toimii lähes kaikilla käyttöjärjestelmillä sekä mobiilialustoilla kuten Android ja iOS. OpenVPN:ää käytettäessä VPN-yhteys muodostetaan koneelle asennettavan ohjelmiston avulla toisin kuin monissa muissa SSL VPN -tekniikalla toteutetuissa järjestelmissä. Sitä pidetään yhtenä turvallisimmista VPN-palveluista maailmassa ja sitä ylläpidetään täysin vapaaehtoisesti käyttäjäyhteisön voimin. OpenVPN:n sivuilla on useita avoimia projekteja, joihin on mahdollista osallistua kuka tahansa. Ensimmäinen versio OpenVPN:stä julkaistiin vuonna 2001 ja kirjoitushetkellä uusin versio on 2.4.6, jota käytetään tässä työssä.

OpenVPN on turvallisempi kuin monet muut VPN-palvelut, sillä se toimii käyttäjäympäristössä (user space), joka mahdollistaa järjestelmän suorittamisen alennetuilla käyttöoikeuksilla (user nobody) ja hiekkalaatikossa (chroot). Monet muut VPN-protokollat toimivat kernelissä. [39.]

8.1 Raspberry Pi:n esivalmistelu

Ennen OpenVPN:n varsinaista asennusta tehdään palvelimelle tarvittavat ja hyödylliset esiasetukset. Ulkoverkossa toimiva VPN-palvelin vaatii porttiohjauksen reitittimeltä, jolloin aukeaa suora yhteys ulkoverkkoon. On suositeltavaa aina konfiguroida laitteen oma palomuuri, kun yhteys ulkoverkkoon avataan, vaikka palvelin sijaitsisi reitittimen palomuurin takana kuten tässä projektissa.

Raspberry Pi:n oma palomuuri ei ole oletuksena päällä, joten se täytyy manuaalisesti aktivoida. Raspbian-käyttöjärjestelmä sisältää muiden Linux-jakeluiden tapaan sisäänrakennetun netfilter-palomuurin, jota konfiguroidaan iptables-käyttöliittymällä. Projektissa kuitenkin käytettiin UFW-käyttöliittymää (Uncomplicated Firewall), koska iptables-käyttöliittymän manuaalinen konfigurointi on hyvin työlästä pitkien komentojen takia. UFW asennetaan komennolla:

sudo apt-get install ufw

Tämän jälkeen aktivoidaan netfilter-palomuuri:

sudo ufw enable

Projektia varten avataan portti 22 SSH-yhteyttä varten, 53 DNS-palvelimelle ja 80 Pi-holen web-käyttöliittymälle. Lisäksi avataan VPN-yhteydelle sen oletusportti 1194 ja määritetään palomuuri sallimaan pelkästään UDP-liikenne. UDP-liikenne on nopeampi verrattuna TCP-liikenteeseen, koska se ei varmista pakettien saapumista.

sudo ufw allow 22
sudo ufw allow 53
sudo ufw allow 80
sudo ufw allow 11555/udp

Lisäturvaksi Raspberry Pi:lle asennetaan myös Fail2ban-tietoturvaohjelma, joka suojaa ensisijaisesti brute force -hyökkäyksiltä. Sen toiminta perustuu yhteyslokien tarkastelemiseen, joista se etsii mahdolliset hyökkäys- ja skannausyritykset verkkoon ja pysäyttää nämä estämällä epäilyttävät IP-osoitteet. Se asennetaan komennolla:

sudo apt-get install fail2ban

Tämän jälkeen Fail2ban aktivoidaan kopioimalla jail.conf -tiedoston sisältö jail.local -tiedostoon.

sudo cp etc/fail2ban/jail.conf /etc/fail2ban/jail.local

Tämän jälkeen luodaan tiedostot openvpn.local ja openvpn, jonne kopioidaan Fail2ban-sivustolta löytyvät oletusasetukset:

sudo nano /etc/fail2ban/filter.d/openvpn.local

```
# Fail2Ban filter for selected OpenVPN rejections
#
#

[Definition]

# Example messages (other matched messages not seen in the testing server's
logs):
# Fri Sep 23 11:55:36 2016 TLS Error: incoming packet authentication failed
from [AF_INET]59.90.146.160:51223
```

```
# Thu Aug 25 09:36:02 2016 117.207.115.143:58922 TLS Error: TLS handshake
failed

failregex = ^ TLS Error: incoming packet authentication failed from
\[AF_INET\]<HOST>:\d+$
            ^ <HOST>:\d+ Connection reset, restarting
            ^ <HOST>:\d+ TLS Auth Error
            ^ <HOST>:\d+ TLS Error: TLS handshake failed$
            ^ <HOST>:\d+ VERIFY ERROR

ignoreregex =
```

sudo nano /etc//jail.d/openvpn

```
# Fail2Ban configuration fragment for OpenVPN

[openvpn]
enabled  = true
port     = 1194
protocol = udp
filter   = openvpn
logpath  = /var/log/openvpn.log
maxretry = 3
```

Tämän jälkeen ohjelma käynnistetään uudelleen komennolla:

sudo service fail2ban restart

8.2 OpenVPN asennus (PiVPN)

OpenVPN-ohjelman asennus tehdään PiVPN-asennusohjelmalla. Se asentaa koneelle OpenVPN:n, luo palvelimelle tarvittavat sertifikaatit ja avaimet. Lisäksi siitä löytyy graafinen käyttöliittymä, jonka avulla konfiguroidaan esiasetukset OpenVPN-palvelimelle. Tämä säästää aikaa, jolloin jokaista asetusta ei tarvitse manuaalisesti käydä muuttamasta OpenVPN:n asennustiedostoista.

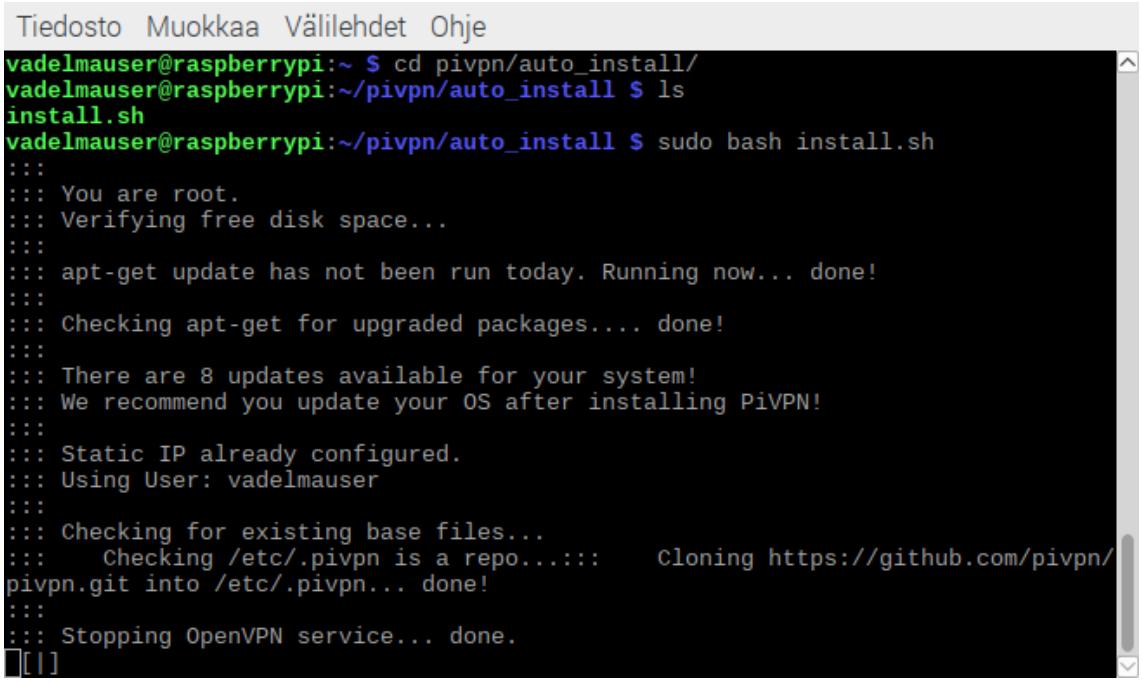
Asennus aloitetaan lataamalla asennuskansio GitHubista:

git clone https://github.com/pivpn/pivpn.git

Tämän jälkeen navigoidaan asennuskansioon ja ajetaan asennusskripti, jonka jälkeen asennusohjelma käynnistyy (ks. kuva 11).

cd pivpn/auto_install/

sudo bash install.sh



Kuva 11. OpenVPN-asennus.

Asennusohjelman aikana määritetään seuraavat asetukset:

- IP-osoite: [Sisäinen-IP-osoite]
- Käyttäjä asennukselle: [Käyttäjä]
- Automaattiset päivitykset: Kyllä
- Valitaan TCP/UDP -protokolla: UDP
- OpenVPN-palvelun porttinumero: [porttinumero]
- ECDSA-salauksen käyttö: Kyllä
- ECDSA-salauksen vahvuus: 256-bit
- Julkisen IP-osoitteen määritys [Julkinen-IP-osoite]
- Valitaan DNS-palvelin 10.8.0.1

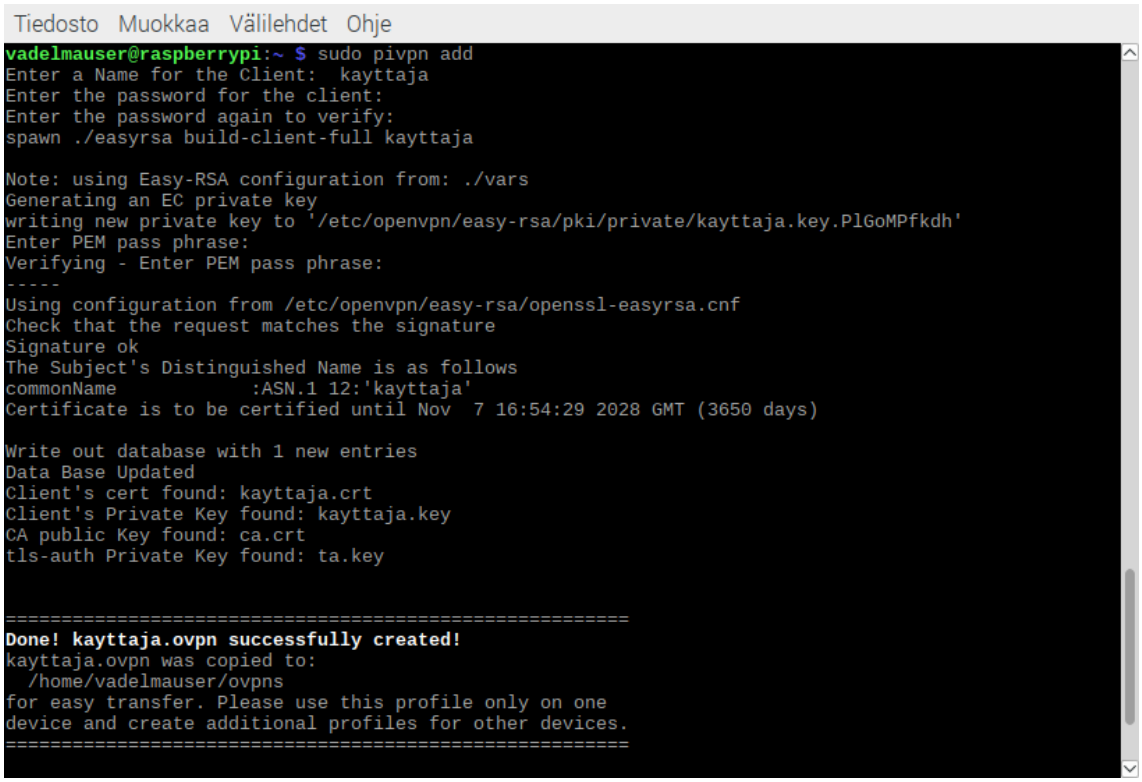
Tämän jälkeen muokataan Pi-holen dnsmasq-ohjelman asetuksia:

sudo nano /etc/dnsmasq.conf

---

listen-address=127.0.0.1, [Sisäinen-IP-osoite], 10.8.0.1

OpenVPN-palvelu on nyt toimintakunnossa. Käyttäjien lisääminen tehdään komennolla pivpn add, jonka jälkeen sille annetaan salasana (ks. kuva 12). On myös mahdollista tehdä käyttäjä ilman salasanaa komennolla pivpn add nopass. OpenVPN-profiilit tallentuvat [käyttäjä].ovpn -nimisenä tiedostona oletuksena kotikansion alle ovpns-kansioon.



Kuva 12. OpenVPN-profiilien luonti.

OpenVPN-sovellus ladataan Androidille Google Play Storesta. Tämän jälkeen laitteelle siirretään aikaisemmin tehty ovpn-tiedosto ja tallennetaan haluttuun paikkaan. Sitten sovellus avataan ja tuodaan tiedosto sovellukseen, jonka jälkeen syötetään aikaisemmin määritetty salasana ja OpenVPN-yhteys on valmis käytettäväksi.

9 Mittaustulokset

Työssä mitattiin Raspberry Pi:n suorituskykyä sen toimiessa OpenVPN-palvelimena sekä testattiin salatun liikenteen suojausta DNS-vuotoja vastaan. Testaukset suoritettiin Android-puhelimilla 3G- ja 4G-verkoissa OpenVPN Connect -sovelluksella. Testauksissa huomioitiin verkkoliikenteen nopeudet sekä yhteyden toimivuus.

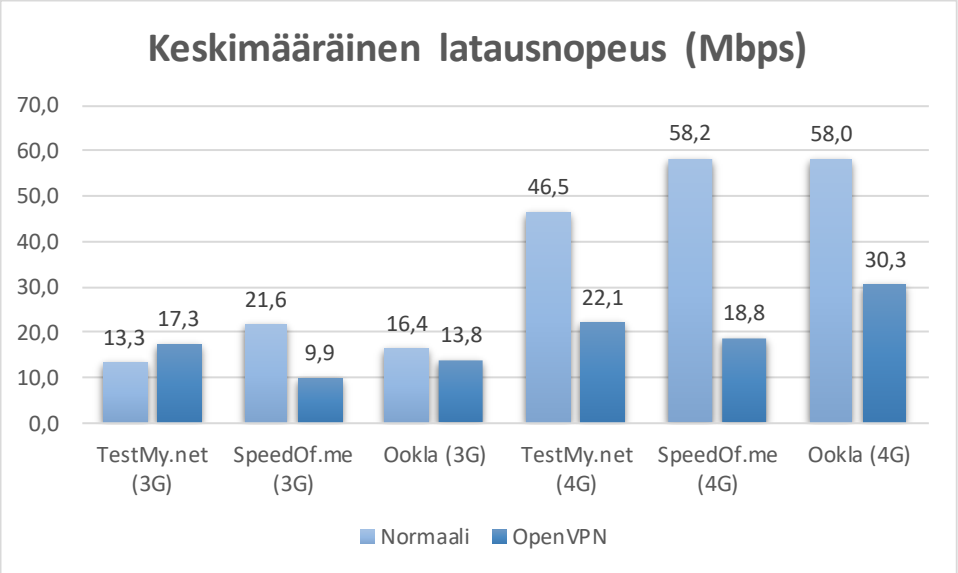
Pi-holen osalta tarkasteltiin Pi-holen tilastoja sekä testattiin yleisimpien verkkosivujen latausaikoja eri laitteilla. Testisivustoiksi valittiin myös sellaisia sivuja, joissa ei ole paljon mainoksia, jotta mittaukset vastaisivat tavanomaista internetin käyttöä. Mittauksia suoritettiin Pi-holen ollessa käytössä sekä mainonnanestolaajennuksen kanssa. Tuloksia vertailtiin tilanteeseen, jossa käytössä ei ole mitään mainonnan- tai seurannanesto-ohjelmaa.

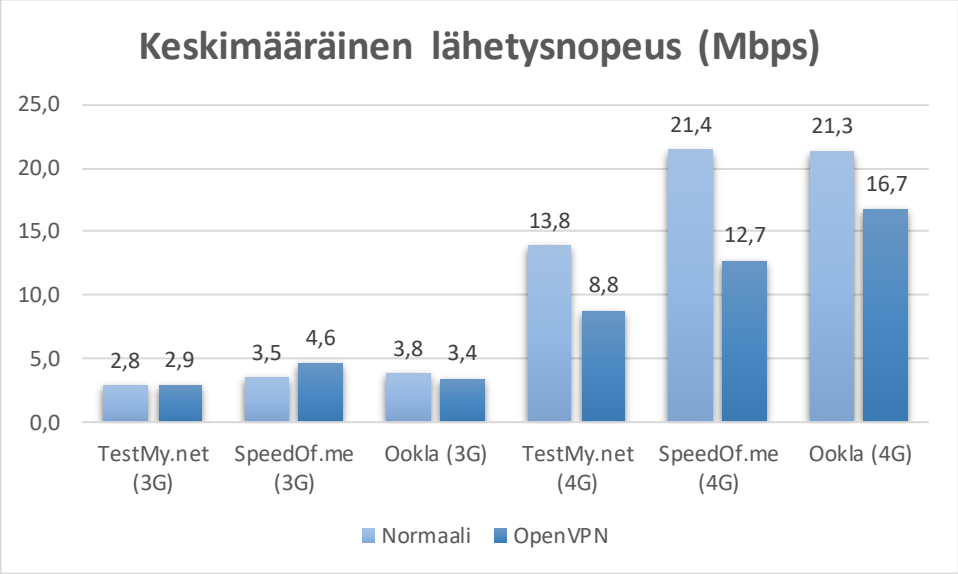
9.1 OpenVPN-palvelimen testaus

OpenVPN-palvelimen nopeutta testattiin vertailemalla kahden eri nopeustestisivuston sekä yhden nopeustestisovelluksen tuloksia keskenään. Testejä suoritettiin viiden päivän ajan eri kellonaikoina ja tuloksista laskettiin keskiarvo. Testisivustoiksi valittiin https://speedof.me/ ja https://testmy.net/. Nopeustestisovelluksena toimi Speedtest by Ookla.

Kuten taulukosta käy ilmi, nopeus hidastui käytettäessä OpenVPN-palvelinta (ks. taulukko 1). Nopeudet kuitenkin pysyivät sellaisina, että pääsääntöisesti normaali internetin käyttö onnistui ilman huomattavaa haittaa. OpenVPN-palvelimessa oli ajoittain havaittavissa 3G-yhteyksillä katkoksia.

Taulukko 1. Lataus- ja lähetysnopeuksien vertailu normaalitilassa ja VPN-palvelimen kanssa.

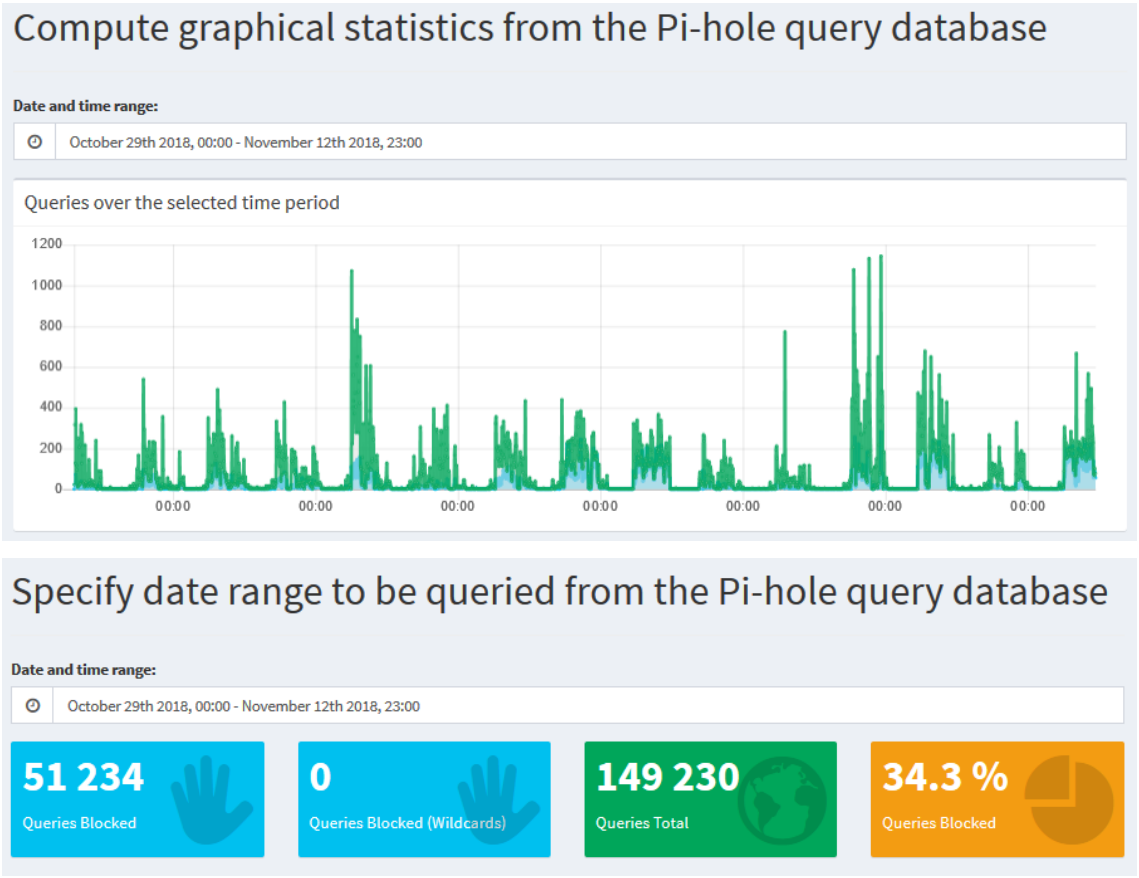




OpenVPN-yhteys todettiin turvalliseksi myös DNS-vuotojen suhteen. Testit suoritettiin sivustoilla https://www.doileak.com/, https://ipleak.net/ ja https://www.dnsleaktest.com/. VPN-palvelua käytettäessä ei todettu DNS-vuotoa.

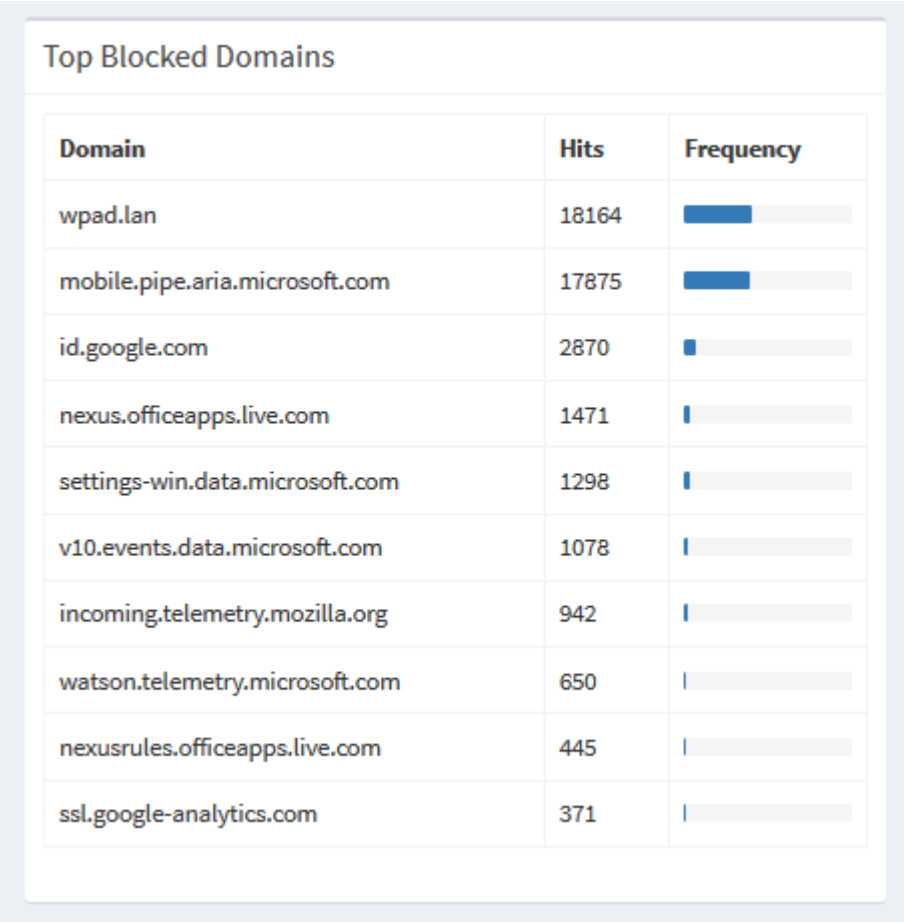
9.2 Pi-holen testaus

Kahden viikon käytön jälkeen tutkittiin Pi-holen tilastoja (ks. kuva 13). Kokonaiskyselyiden määrä oli 149 230, joista estettyjä oli 51 234 eli 34,3 %.



Kuva 13. Pi-holen DNS-kyselyiden kokonaismäärä kahden viikon ajalta.

Estettyjen kyselyiden määrä oli yllättävän korkea ja tutkittaessa asiaa huomattiin, että kaksi isointa estettyä verkkotunnusta olivat mobile.pipe.aria.microsoft.com ja wpad.lan huomattavan suurella osuudella. Niitä oli estetty yhteensä 36 039 kertaa (ks. kuva 14). Lisäselvityksissä huomattiin, että kyseiset DNS-pyynnöt liittyivät WPAD-kyselyihin (Web Proxy Auto-Discovery Protocol) sekä Skypen, Onedriven tai Outlookin toimintaan.



Top Blocked Domains

Domain	Hits	Frequency
wpad.lan	18164	
mobile.pipe.aria.microsoft.com	17875	
id.google.com	2870	
nexus.officeapps.live.com	1471	
settings-win.data.microsoft.com	1298	
v10.events.data.microsoft.com	1078	
incoming.telemetry.mozilla.org	942	
watson.telemetry.microsoft.com	650	
nexusrules.officeapps.live.com	445	
ssl.google-analytics.com	371	

Kuva 14. Yleisimmät estetyt verkkotunnukset.

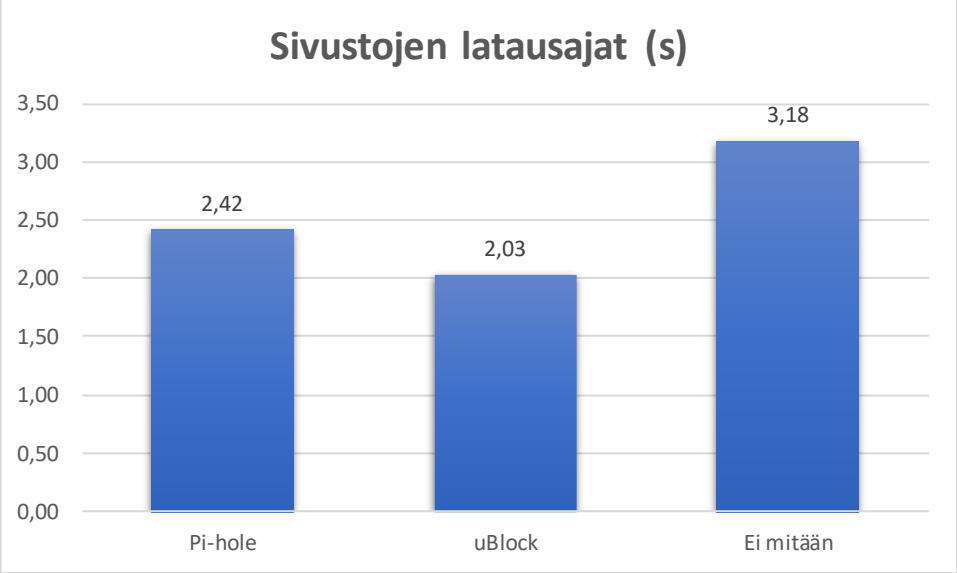
Lopputuloksissa tämäntyyppiset DNS-pyynnöt päätettiin olla huomioimatta, koska tarkoituksena oli mitata mainonnan- ja seurannanestoa sekä sovellusten telemetrialiikennettä. DNS-kyselyiden kokonaismääräksi jäi 108522 kyselyä, joista estettyjä oli 15295, eli 14,1 %. Tämä tarkoittaa, että kahden viikon aikana 14,1 % verkkoliikenteestä koostui sivustojen kautta tapahtuvasta seurannasta ja mainonnasta sekä eri sovellusten lähettämistä telemetriatiedoista.

Pi-holen osalta vertailtiin kymmenen eri sivuston latausaikoja viiteen kertaan mitattuna. Mittaukset toteutettiin Chrome-selaimella oletusasetuksilla sisäänrakennetun mainonnaneston ollessa kytkettynä pois päältä. Testit suoritettiin kolmessa eri tilassa:

- Laitteelle ei ollut asennettu mainonnan- tai seurannanesto-ohjelmia ja Pi-hole oli kytketty pois päältä.
- Laitteelle ei ollut asennettu mainonnan- tai seurannanesto-ohjelmia ja Pi-hole oli kytketty päälle.
- Laitteelle oli asennettu mainonnanestolaajennus ja Pi-hole oli kytketty pois päältä.

Testeissä havaittiin, että uBlock-laajennuksella keskimääräinen sivujen latausaika oli 2,03 sekuntia. Pi-holella keskimääräinen latausaika oli 2,42 sekuntia, eli 0,39 sekuntia hitaampi kuin uBlock-laajennuksella. Sivujen latausaika oli odotetusti hitain, 3,18 sekuntia, ilman mitään seurannan- tai mainonnanesto-ohjelmaa (ks. taulukko 2).

Taulukko 2. Sivustojen latausaikojen vertailu.



Mittauksissa haluttiin ensisijaisesti tutkia Pi-holen vaikutusta käytetyn datan määrään ja sivujen latausaikoihin. Jos on olennaista säästää datan käyttöä saavuttaakseen parhaimman kokonaistuloksen, kannattaa käyttää Pi-holen sekä halutun mainonnanesto-laajennuksen yhdistelmää.

Pi-holen nopeus paranee käytön myötä sen tallentaessa verkkotunnuksia välimuistiinsa. Lisäksi estolistojen päivityksillä voidaan jatkuvasti parantaa sen suorituskykyä.

10 Loppuhuomioita

Tämän insinöörityön tavoitteena oli tutkia erilaisia seurantamenetelmiä ja yksityisyyden toteutumista internetissä sekä toteuttaa oman kotiverkon liikenteen suojaus. Seurantamenetelmiin perehtyessä selvisi, että seuranta on erittäin laaja-alaista ja siltä on lähes mahdotonta suojautua kokonaan. Yksityisyydelle luovat uhan myös tietojenkalasteluyritykset sekä haittaohjelmat, kuten erilaiset kiristys- ja vakoiluohjelmat. Tässä työssä kuitenkin haluttiin keskittyä käyttäjän seurantaan ja siihen, kuinka huomaamattomasti se tapahtuu.

Mitä pidemmälle tutkimus erilaisista seurannan menetelmistä eteni, sitä useammin vastaan tuli yritysten argumentti, että tietoja kerätään vain palvelun parantamiseksi. Tämä varmaankin pitää paikkansa. Yrityksiä ei varsinaisesti kiinnosta yksittäisten ihmisten yksittäiset toiminnot. Yrityksen kannalta palvelun parantaminen tarkoittaa palvelun kehittämistä niin, että saadaan uusia asiakkaita tai käyttäjiä, eivätkä vanhat karkaa kilpailijoille. Usein yritysten toiminta kuitenkin loukkaa ihmisten oikeutta yksityisyyteen ja sen takia onkin oltava jatkuvasti valppaana ja pitää huolta oikeuksistaan.

Yksityisyyden suojaaminen ei onnistu vain yksittäisillä teoilla, vaan useiden eri suojautumismenetelmien yhdistelmällä. Tämä tarkoittaakin, että suojausta kannattaa ajatella monitasoisena asiana, jossa ei voi luottaa vain yhteen ratkaisuun. Teknologia kehittyy jatkuvasti, ja tällä hetkellä toimivat suojaukset saattavat olla tehottomia tulevaisuudessa.

Insinöörityöprosessin aikana selvisi, että julki tulleita tapauksia, joissa yksityisyydensuojaa oli rikottu, oli paljon enemmän, kuin aluksi ajateltiin. Kuitenkin moni näistä tapauksista ei ollut saanut niin suurta huomiota, kuin olisi odottanut. Tämä saattaa johtua siitä, että seurannasta on tullut niin tavallista, ettei se enää yllätä ketään.

Kotiverkon ja siihen liitettyjen laitteiden suojaus onnistui tavoitteiden mukaisesti. Tarkoituksena oli kuitenkin valita ns. kultainen keskitie käytettävyyden ja yksityisyyden suhteen. Hankaluutta aiheutti erilaisten toteutusmahdollisuuksien ja tapojen runsaus sekä aiheen rajaus.

Lähteet

1 Schneier, Bruce. 2015. Data and Goliath: The Hidden Battles to Collect Your Data & Control Your World. New York: W. W. Norton & Company.

2 Cadwalladr, Carole & Graham-Harrison, Emma. 2018. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. Verkkoaineisto. The Guardian. < https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>. Luettu 3.10.2018.

3 Neate, Rupert. 2018. Over $119bn wiped off Facebook's market cap after growth shock. Verkkoaineisto. The Guardian. <https://www.theguardian.com/technology/2018/jul/26/facebook-market-cap-falls-109bn-dollars-after-growth-shock>. Luettu 3.10.2018.

4 Canon, Gabrielle. 2018. Facebook growth slows as Zuckerberg says developed countries are saturated. Verkkoaineisto. The Guardian. <https://www.theguardian.com/technology/2018/oct/30/facebook-quarterly-report-revenue-growth>. Luettu 9.11.2018.

5 Rathnam, Lavanya. 2018. PRISM, Snowden and Government Surveillance: 6 Things You Need To Know. Verkkoaineisto. Cloudwards. <https://www.cloudwards.net/prism-snowden-and-government-surveillance/>. Luettu 7.10.2018.

6 Daniel, Ellen. 2018. Five years on, what has changed since the Edward Snowden scandal?. Verkkoaineisto. Verdict. <https://www.verdict.co.uk/snowden-scandal-five-years-gdpr/>. Luettu 8.10.2018.

7 Vänskä, Olli. 2018. Kiina alkoi ”pisteyttää” kansalaisiaan: pohjasakka ei saa ostaa edes juna- tai lentolippuja. Verkkoaineisto. Mikrobitti <https://www.mikrobitti.fi/uutiset/kiina-alkoi-pisteyttaa-kansalaisiaan-pohjasakka-ei-saa-ostaa-edes-juna-tai-lentolippuja/bfbd5504-0ae7-375e-b8f2-227bef41751b>. Luettu 6.10.2018.

8 Hallamaa, Teemu & Lyytikkä, Jyrki. 2018. Kiina rakentaa verkkoa maailmalle – Googlen ex-toimitusjohtaja ennustaa, että Kiinan vaikutusvallan kasvu jakaa internetin kahtia. Verkkoaineisto. YLE. <https://yle.fi/uutiset/3-10442069>. Luettu 12.10.2018

9 Hänninen, Kari. 2014. Ukkoverkot valitsi Huawein kumppanikseen verkoissa. Verkkoaineisto. Kauppalehti. <https://www.kauppalehti.fi/uutiset/ukkoverkot-valitsi-huawein-kumppanikseen-verkoissa/4623ab4e-d14d-3c83-b367-6e271e13d979>. Luettu 12.10.2018.

10 Poliisi yrittää hillitä henkilökunnan uteliaisuutta uusin keinoin urkintaskandaalien jälkeen. 2016. Verkkoaineisto. MTVuutiset. <https://www.mtv.fi/uutiset/kotimaa/artikkeli/poliisissa-jatkotoimia-myllyla-ja-auer-urkintaskandaalien-jalkeen/6069886#gs> Luettu 8.10.2018.

11 Reinboth, Susanna. 2014. Luvan puhelinkuunteluun voi saada kevyin perustein. Verkkoaineisto. Helsingin Sanomat. <https://www.hs.fi/kotimaa/art-2000002757694.html>. Luettu 10.10.2018.

12 Gayle, Everton. 2018. Google tracks your every move. Verkkoaineisto. Euronews. <https://www.euronews.com/2018/08/14/google-knows-everywhere-you-go>. Luettu 8.11.2018.

13 Kiss, Jemima. 2010. Google admits collecting Wi-Fi data through Street View cars. Verkkoaineisto. The Guardian. <https://www.theguardian.com/technology/2010/may/15/google-admits-storing-private-data>. Luettu 8.11.2018.

14 Google faces Streetview wi-fi snooping action. Verkkoaineisto. BBC. <https://www.bbc.com/news/technology-24047235>. Luettu 8.11.2018.

15 Gallagher, Ryan. 2018. Google Plans to Launch Censored Search Engine in China, Leaked Documents Reveal. Verkkoaineisto. The Intercept. <https://theintercept.com/2018/08/01/google-china-search-engine-censorship/>. Luettu 8.11.2018.

16 Shrivastava, Parth. 2018. All you need to know about GDPR—Explained. Verkkojulkaisu. Hackernoon. <https://hackernoon.com/all-you-need-to-know-about-gdpr-explained-8e336a1987ea>. Luettu 27.10.2018.

17 Budington, Bill & Szymielewicz, Katarzyna. 2018. The GDPR and Browser Fingerprinting: How It Changes the Game for the Sneakiest Web Trackers. Verkkoaineisto. EFF. <https://www.eff.org/deeplinks/2018/06/gdpr-and-browser-fingerprinting-how-it-changes-game-sneakiest-web-trackers>. Luettu 8.11.2018.

18 Dignan, Larry. 2012. Mac users pay more than PC users, says Orbitz. Verkkoaineisto. Cnet. <https://www.cnet.com/news/mac-users-pay-more-than-pc-users-says-orbitz/>. Luettu 8.11.2018.

19 Arns, Tobias. 2018. The New Paywall Is Dymanic: How the Wall Street Journal Grew Subscriptions by 25 Percent. Verkkoaineisto. Cxense. <https://www.cxense.com/blog/new-paywall-bendable-how-wall-street-journal-re-defined-paywall-and-how-you-can-grow>. Luettu 8.11.2018.

20 How Canvas Fingerprint Blockers Make You Easily Trackable. 2016. Verkkoaineisto. Multilogin.com <https://multilogin.com/how-canvas-fingerprint-blockers-make-you-easily-trackable/>. Luettu 8.11.2018.

21 Fortuna, Andrea. 2017. What is Canvas Fingerprinting and how the companies use it to track you online. Verkkoaineisto. Andreafortuna.com. <https://www.andreafortuna.org/cybersecurity/privacy/what-is-canvas-fingerprinting-and-how-the-companies-use-it-to-track-you-online/>. Luettu 8.11.2018.

22 WebGL Browser Report. Verkkoaineisto <https://browserleaks.com/webgl>. Luettu 8.11.2018.

23 AudioContext Fingerprinting. 2017. Verkkoaineisto. Darkwave Technologies. <https://www.darkwavetech.com/index.php/device-fingerprint-blog/audiocontext-fingerprinting>. Luettu 7.11.2018.

24 Kamkar, Samy. Evercookie. Verkkoaineisto. GitHub <https://github.com/samyk/evercookie>. Luettu 9.11.2018.

25 Locklear, Mallory. 2018. Google responds to lawmaker concerns over Gmail scanning. Verkkoaineisto. Engadget. <https://www.engadget.com/2018/09/20/google-lawmaker-concerns-gmail-scanning/>. Luettu 9.11.2018.

26 Perlroth, Nicole. 2016. Yahoo Says Hackers Stole Data on 500 Million Users in 2014. Verkkoaineisto. The New York Times. <https://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html>. Luettu 9.11.2018

27 Morris, Scott. 2018. Tech 101: What is a Tracking Pixel?. Verkkoaineisto. Skillcrush. <https://skillcrush.com/2012/07/19/tracking-pixel/>. Luettu 12.10.2018.

28 Dascalescu, Ana. 2018. Doxxing Can Ruin Your life. Here's How (You Can Avoid It). Verkkoaineisto. Heimdal Security. <https://heimdalsecurity.com/blog/doxxing/>. Luettu 13.10.2018.

29 Patterson, Richard. 2017. VPN statistics: What the numbers tell us about VPNs. Verkkoaineisto. Comparitech. <https://www.comparitech.com/vpn/vpn-statistics/>. Luettu 6.11.2018.

30 Degree of internet freedom in selected countries according to the Freedom House Index 2018. 2018. Verkkoaineisto. Statista. <https://www.statista.com/statistics/272533/degree-of-internet-freedom-in-selected-countries/>. Luettu 6.11.2018.

31 What is VPN encryption and why it is important? 2018. Verkkoaineisto. CactusVPN. <https://www.cactusvpn.com/beginners-guide-to-vpn/vpn-encryption/>. Luettu 1.11.2018.

32 Taylor, Sven. 2018. VPN Tests and Checks. Verkkoaineisto. Restore Privacy. <https://restoreprivacy.com/vpn-test/>. Luettu 1.11.2018.

33 Viljanen Vesa. Anonyymit verkot. Verkkoaineisto. Yksityisyydensuoja.fi <https://www.yksityisyydensuoja.fi/content/anonyymit-verkot>. Luettu 2.11.2018.

34 Tor-projektin kotisivu. Verkkoaineisto <https://www.torproject.org/index.html.en>. Luettu 5.11.2018.

35 Proton Technologies. Verkkoaineisto <https://protonmail.com/>. 29.10.2018.

36 Raspberry Pi Foundation. Verkkoaineisto. <https://www.raspberrypi.org/>. Luettu 9.10.2018.

37 Pi-hole. Verkkoaineisto. <https://pi-hole.net/>. Luettu 11.10.2018.

38 Telekrmor. 2018. Verkkoaineisto. <https://pi-hole.net/2018/02/02/why-some-pages-load-slow-when-using-pi-hole-and-how-to-fix-it/>. Luettu 11.10.2018.

39 OpenVPN. Verkkoaineisto. <https://community.openvpn.net/openvpn/wiki>. Luettu 16.10.2018.

OpenVPN-palvelimen nopeustestit

LATAUS	30.10.18	31.10.18	1.11.18	2.11.18	3.11.18	KESKIARVO
TestMy.net (3G)	22,3	8,6	14,4	11,1	10,3	13,3
SpeedOf.me (3G)	24,5	20,9	20,3	22,8	19,3	21,6
Ookla (3G)	14,0	20,8	13,6	17,5	16,0	16,4
TestMy.net (4G)	47,3	45,3	33,9	47,2	58,6	46,5
SpeedOf.me (4G)	65,9	53,4	65,2	65,2	41,4	58,2
Ookla (4G)	71,3	58,4	57,1	55,7	47,7	58,0
LÄHETYS						
TestMy.net (3G)	3,4	2,5	2,1	3,2	3,0	2,8
SpeedOf.me (3G)	3,7	3,1	3,8	3,7	3,1	3,5
Ookla (3G)	3,6	4,1	3,2	4,3	3,9	3,8
TestMy.net (4G)	9,9	19,9	5,0	18,4	15,9	13,8
SpeedOf.me (4G)	12,7	18,1	38,8	19,6	17,8	21,4
Ookla (4G)	14,4	25,1	25,2	25,4	16,5	21,3
LATAUS VPN						
TestMy.net (3G)	20,8	20,5	6,8	19,2	19,4	17,3
SpeedOf.me (3G)	10,6	10,5	9,8	10,0	8,6	9,9
Ookla (3G)	11,4	13,3	15,9	13,9	14,5	13,8
TestMy.net (4G)	21,9	18,8	23,6	24,4	21,8	22,1
SpeedOf.me (4G)	18,2	21,2	15,4	20,2	19,0	18,8
Ookla (4G)	40,0	20,4	29,4	38,5	23,4	30,3
LÄHETYS VPN						
TestMy.net (3G)	2,8	3,0	2,9	2,8	3,1	2,9
SpeedOf.me (3G)	6,6	3,7	3,8	3,8	5,2	4,6
Ookla (3G)	2,6	3,5	3,9	3,5	3,7	3,4
TestMy.net (4G)	9,0	9,1	8,0	8,5	9,3	8,8
SpeedOf.me (4G)	14,3	12,6	11,3	12,2	13,1	12,7
Ookla (4G)	18,6	14,7	18,3	18,7	13,2	16,7