Pinja Parviainen

Sormenjälkitunnistus internetin käyttäjien seuraamisteknologiana

Tietotekniikan kandidaatintutkielma

30. huhtikuuta 2021

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Pinja Parviainen

Yhteystiedot: pinja.k.parviainen@student.jyu.fi

Ohjaaja: Antti-Jussi Lakanen

Työn nimi: Sormenjälkitunnistus internetin käyttäjien seuraamisteknologiana

Title in English: Browser fingerprinting as user tracking technology

Työ: Kandidaatintutkielma

Opintosuunta: Tietotekniikka

Sivumäärä: 25+0

Tiivistelmä: Tutkimuksessa tutkitaan sormenjälkitunnistusta käyttäjän yksityisyyden näkökulmasta. Tutkimuskysymyksiin kuuluu muun muassa: voiko sormenjälkitunnistuksella seuraamista estää ja kuinka moni sivusto käyttää sormenjälkitunnistusta. Tutkimus on suoritettu kirjallisuuskatsauksena.

Avainsanat: Sormenjälkitunnistus, Yksityisyys, Käyttäjien seuraaminen, Kandidaatintutkielma, Kirjallisuuskatsaus

Abstract: The main motive for this study is to look at browser fingerprinting from the perspective of the user's privacy. The research questions include among others: can you prevent tracking by browser fingerprinting and how many sites use browser fingerprinting. The study is a literary review.

Keywords: Browser fingerprinting, Privacy, Tracking users, Bachelor's Theses, Literary review

Sisällys

1 JOHDANTO 1

2 SORMENJÄLKITUNNISTUS 3

2.1 Yleistä sormenjälkitunnistuksesta ..... 3 2.2 HTTP-sormenjälki 4

2.3 JavaScript-sormenjälki 4
2.4 Lisäosat ja laajennukset 5

3 SORMENJÄLKITUNNISTUKSEN HUOMAAMISESTA 7

4 SORMENJÄLKITUNNISTUKSEN TOIMIVUUDESTA 9

5 MIKSI SORMENJÄLKITUNNISTUS ON UHKA YKSITYISYYDELLE 11

6 SORMENJÄLKITUNNISTUSTA VASTAAN SUOJAUTUMINEN 13
6.1 Yleistä suojautumisesta 13
6.2 Laajennukset.....14
6.3 Tor-selain 15
6.4 Brave-selain 16
6.5 Muut 16

7 YHTEENVETO.....18

LÄHTEET 20

1 Johdanto

Sormenjälkitunnistus on tekniikka, jonka avulla voidaan seurata käyttäjiä verkossa muodostamalla jokaiselle käyttäjälle oma yksilöllinen tunnus, niin sanottu sormenjälki. Käyttäjästä kerätään erilaisia helposti saatavilla olevia tietoja, kuten selaimen versio, kieli, laajennukset ja laitteen käyttöjärjestelmä. Nämä yhdessä muodostavat muista käyttäjistä eroavan kokonaisuuden.

Tutkimuksen tarkoitus on tarkastella sormenjälkitunnistusta käyttäjän yksityisyyden näkökulmasta. Tutkimuksessa tarkastellaan mitä sormenjälkitunnistus on, miten se toimii ja onko se uhka käyttäjien yksityisyydelle. Tutkimuksessa pyritään vastaamaan seuraaviin tutkimuskysymyksiin:

- Kuinka moni sivusto käyttää sormenjälkitunnistusta?
- Kuinka hyvin sormenjälkitunnistuksella saadaan yksilöityä käyttäjät?
- Mistä tietää käyttääkö sivusto sormenjälkitunnistusta?
- Onko sormenjälkitunnistuksella seuraamista mahdollista estää?

Tutkimus antaa hyvän yleiskuvan aiheesta, vaikka lukija ei entuudestaan tuntisi aihetta, mutta tutkimuskysymysten avulla pystyy syventymään aiheeseen tarkasti. Tutkimuskysymykset liittyvät kaikki toisiinsa, joten aihe pysyy hyvin rajattuna, eikä tutkimus pitene loputtomasti.

Aihe on käytännön kannalta tärkeä, sillä tutkimuksen määrästä huolimatta sormenjälkitunnistus on aiheena suhteellisen tuntematon. Vasta viimeisen vuoden aikana on sormenjälkitunnistuksen tietoisuus noussut sen verran, että osa suuremmista selaimista on tehnyt toimenpiteitä sen estämiseen. Sormenjälkitunnistuksen käyttö on koko ajan lisääntymässä ja uusia tehokkaampia keinoja kehitetään jatkuvasti (Al-Fannah ja Mitchell 2020), joten tietoisuuden lisääminen aiheesta on internetin käyttäjien yksityisyyden kannalta välttämätöntä.

Tutkimus toteutettiin kirjallisuuskatsauksena. Lähteet haettiin Google Scholarista erilaisilla sormenjälkitunnistukseen liittyvillä hauilla, kuten "detecting browser fingerprinting", "web

browser tracking technology"ja "browser fingerprinting techniques". Lähteissä suosittiin uudempia lähteitä, sillä sormenjälkitunnistus tekniikkana muuttuu ja uudistuu jatkuvasti. Vanhoissa tutkimuksissa on helposti vanhentunutta tietoa. Vanhempia tutkimuksia otettiin kuitenkin mukaan tutkimuksen lähteiksi, mikäli niiden tiedot olivat edelleen ajan tasalla.

Tutkimus koostuu johdannosta, kuudesta käsittelykappaleesta ja yhteenvedosta. Luvussa kaksi käsitellään yleisesti sormenjälkitunnistusta ja sen toimintaa. Luvun on tarkoitus esitellä lukijalle mitä sormenjälkitunnistus on ja miten se toimii. Luvussa kolme syvennytään sormenjälkitunnistuksen tunnistamiseen verkkosivuilla. Luku esittelee, miten sormenjälkitunnistus on mahdollista huomata. Luvussa neljä käsitellään sormenjälkitunnistuksen toimivuutta, eli sitä kuinka hyvin sillä saadaan yksilöityä käyttäjät. Luvussa viisi tarkastellaan sormenjälkitunnistusta uhkana käyttäjien yksityisyydelle. Tarkoituksena on esitellä lukijalle syitä, miksi sormenjälkitunnistusta halutaan estää. Luvussa kuusi tutkitaan voiko sormenjälkitunnistusta estää ja käsitellään eri tekniikoita sormenjälkitunnistuksen estämiseen.

2 Sormenjälkitunnistus

2.1 Yleistä sormenjälkitunnistuksesta

Sormenjälkitunnistus esiteltiin ensimmäisen kerran tieteellisessä tutkimuksessa vuonna 2009, jolloin Mayer (2009) todisti sormenjälkitunnistuksen toimivan luomalla sormenjäljen 96 %:lle 1300 käyttäjästä (Mayer 2009). Seuraavana vuonna Eckersley (2010) teki ensimmäisen laajamuotoisen tutkimuksen aiheeseen. Hänen tutkimuksessaan kerättiin yli 470 000 tietokoneen tiedot ja pyrittiin yksilöimään kaikki sormenjälkitunnistuksella. Tutkimuksessa onnistuttiin luomaan yksilöllinen sormenjälki 83,6 % käyttäjistä (Eckersley 2010).

Sormenjälkitunnistusta käytetään pääasiassa kohdennettuun mainontaan ja käyttäjien seuraamiseen (Englehardt ja Narayanan 2016; Al-Fannah, Li ja Mitchell 2018), mutta lisäksi sillä on muitakin käyttötapoja. Sormenjälkitunnistusta voidaan esimerkiksi käyttää käyttäjien todentamiseen salasanojen rinnalla (Andriamilanto, Allard ja Guelvouit 2021) ja bottien tunnistamiseen (Li ja Cao 2020).

Yhä useampi käyttäjä käyttää erilaisia yksityisyyttä suojaavia lisäosia ja kieltäytyy evästeistä (Gómez-Boix, Laperdrix ja Baudry 2018). Tämän takia käyttäjien seuraaminen evästeillä on koko ajan haastavampaa. On esitetty, että tämä loi tarpeen uusille tehokkaammille tavoille seurata käyttäjiä verkossa (Nikiforakis ym. 2013). Kun sormenjälkitunnistus tekniikkana sai tietoisuutta, nousi sen käyttö reaalimaailmassa nopeasti (Al-Fannah, Li ja Mitchell 2018). Vuonna 2013 vain 0,4 % suosituimmasta 10 000 verkkosivusta käytti sormenjälkitunnistusta (Acar ym. 2013), kun taas vuonna 2018 suosituimmasta 10 000 verkkosivusta 68,8 % käytti sormenjälkitunnistusta jollain tasolla (Al-Fannah, Li ja Mitchell 2018).

Suosituista verkkosivuista esimerkiksi Skype (Nikiforakis ym. 2013), Google (Al-Fannah, Li ja Mitchell 2018) ja Facebook (Englehardt ja Narayanan 2016) käyttävät sormenjälkitunnistusta. Al-Fannah, Li ja Mitchell (2018) mukaan yleisin sormenjälkitunnistusta tarjonnut kolmas osapuoli oli Google analytics.

Sormenjälkitunnistusta Google analyticsin toimesta löydettiin 58 % suosituimmista verkkosivuista (Al-Fannah, Li ja Mitchell 2018).

Sormenjälki voidaan luoda käyttämällä monia eri tietoja ja nämä tiedot on mahdollista kerätä käyttäjästä monella tapaa. Tämän ansiosta on olemassa monia erilaisia tekniikoita sormenjälkitunnistuksen toteuttamiseen. Eri tekniikat voidaan jakaa karkeasti passiivisiin ja aktiivisiin tekniikoihin (Adamsky, Schiffner ja Engel 2020). Passiiviset sormenjälkitunnistustekniikat hyödyntävät jo vapaasti saatavilla olevaa tietoa, eivätkä vaadi tiedon keräämistä erillisiä kyselyitä käyttäen (Al-Fannah ja Mitchell 2020). Aktiiviset sormenjälkitunnistustekniikat taas vaativat, että haluttua tietoa kysellään käyttäjän laitteelta jollain tapaa (Adamsky, Schiffner ja Engel 2020).

2.2 HTTP-sormenjälki

HTTP-sormenjälki muodostetaan passiivisesti hyödyntämällä selaimen ja palvelimen välisiä tavanomaisia HTTP-kyselyitä (Al-Fannah ja Mitchell 2020). Sormenjälki luodaan käyttämällä HTTP-kyselyiden otsikkokenttiä (Kaur ym. 2017), jotka selain antaa palvelimelle verkkosivujen näyttämistä ja toimintaa varten. Ilman näitä otsikkokenttien sisältämiä tietoja verkkosivustot eivät toimisi oikein.

Sormenjäljen muodostamiseen HTTP:n avulla siis riittää, että käyttäjä avaa verkkosivun, joka käyttää sormenjälkitunnistusta. Käyttäjälle sormenjäljen muodostuminen ei näy mitenkään, eikä sormenjälkitunnistusta käyttävän verkkosivun avaaminen eroa muista verkkosivuista mitenkään.

HTTP-otsikkokentillä sormenjälkeä varten käyttäjästä saadaan kerättyä esimerkiksi IP-osoite, user-agent, laitteen käyttöjärjestelmä ja kielet, sekä selaimen tiedot (Kaur ym. 2017). Näistä sormenjäljen muodostuksen kannalta tärkein on user-agent. Koska user-agent tietueessa on käyttäjien välillä eniten eroavaisuuksia (Li ja Cao 2020), tulee tämän tiedon sisältävästä sormenjäljestä todennäköisemmin yksilöllinen. User-agentin avulla käyttäjät pystytään erottamaan toisistaan jopa saman IP-osoitteen sisällä (Kaur ym. 2017).

2.3 JavaScript-sormenjälki

JavaScript-sormenjälki luodaan aktiivisesti esittämällä käyttäjälle näkymättömiä kyselyitä käyttäjän laitteelle (Adamsky, Schiffner ja Engel 2020). Kyselyillä tarkoitetaan tilannetta, jossa palvelin lähettää selaimelle tietyn JavaScript-koodin, johon selain vastaa (Adamsky, Schiffner ja Engel 2020). Kyselyt toteutetaan lisäämällä sivuston JavaScript-koodiin koodipätkä, joka suorittaa kyselyn (Al-Fannah, Li ja Mitchell 2018). Tällä tapaa käyttäjän laitteesta saadaan selvitettyä esimerkiksi laitteen näytön tiedot, laitteen fontit ja sivuhistoria (Acar ym. 2013). Laitteen fontit ja näytön koko ovat yksiä hyödyllisimmistä tiedoista sormenjälkitunnistuksen kannalta (Kaur ym. 2017; Bujlow ym. 2017).

Kaikki modernit selaimet tukevat JavaScriptia (Acar ym. 2013) ja lähes kaikki verkkosivut käyttävät sitä (K. V. Nair 2018). Hyvin harvat muut kuin staattiset verkkosivut eivät käytä JavaScriptia (Acar ym. 2013), sillä sitä käytetään verkkosivujen eri toimintoihin. JavaScript on niin olennainen osa verkkosivujen toimintaa, että vain 1 % käyttäjistä estää sen (Kaur ym. 2017).

JavaScriptiä hyödyntämällä on mahdollista luoda laitekohtainen, selaimesta riippumaton sormenjälki (Eng. Cross Browser Fingerprint) (Bujlow ym. 2017). Tällainen sormenjälki mahdollistaa käyttäjän tunnistamisen ja seuraamisen, vaikka tämä vaihtaisi selainta (K. V. Nair 2018). Selaimesta riippumattoman sormenjäljen luomiseen käytetään ainoastaan laitekohtaisia tietoja, eikä esimerkiksi tietoja selaimesta (Bujlow ym. 2017). Laitekohtaisia tietoja ovat esimerkiksi näytön koko, käyttöjärjestelmä ja fontit.

2.4 Lisäosat ja laajennukset

Laajennukset ja lisäosat ovat selaimeen ladattavia ohjelmistoja, jotka tarjoavat lisäominaisuuksia selaimeen. Selaimen laajennukset ovat yksi tehokkaimmista tavoista luoda sormenjälki (Kaur ym. 2017). Mitä useampia laajennuksia lataa, sitä yksilöllisempi sormenjälki käyttäjällä on (K. V. Nair 2018).

JavaScriptillä ei pääse käsiksi listaan siitä, mitä laajennuksia käyttäjällä on selaimellaan, vaan laajennusten olemassaolon huomaa vain niiden vaikutuksesta verkkosivuun (Nikiforakis ym. 2013). Esimerkiksi jos selain ei näytä mainoksia, tiedetään että käyttäjällä on jonkunlainen mainosten-esto-laajennus. Laajennusten olemassaoloa selvitetään kokeilemalla (Acar ym. 2013).

Kokeilu suoritetaan asettamalla verkkosivuston erilaisia JavaScript-koodeja tätä tarkoitusta varten ja tarkastelemalla suoritettiinko kyseiset koodit onnistuneesti (Acar ym. 2013). Tarkastelemalla mitkä koodit toimivat ja mitkä eivät, voidaan päätellä mitä laajennuksia selaimeen on ladattu (Nikiforakis ym. 2013). Esimerkiksi erilaisien mainosten esto-laajennusten olemassaolon huomaa, jos mainosten näyttämiseen käytettyjä koodeja ei suoritettu onnistuneesti (Nikiforakis ym. 2013).

Lisäosat olivat aiemmin yksi tehokkaimpia tapoja luoda sormenjälki (Laperdrix ym. 2020), mutta nykyään Google Chrome ei enää tue NPAPI-teknologiaa (Netscape Plugin Application Programming Interface), eikä tätä kautta lisäosiakaan (Schuh 2013). Muutkaan suuremmat selaimet, kuten Firefox ja Safari, eivät enää tue lisäosia (Laperdrix ym. 2020). Selaimilla, jotka eivät tue lisäosia ei ole mahdollista luoda sormenjälkeä lisäosia käyttämällä.

Lisäosien kautta pääsi JavaScriptin tavoin käsiksi laitteen ominaisuuksiin, kuten fontteihin (Acar ym. 2013). Myös tietoa siitä, mitä lisäosia selaimeen oli ladattu, on käytetty sormenjälkitunnistuksessa (Kaur ym. 2017) samalla tavalla kuin laajennuksiakin.

3 Sormenjälkitunnistuksen huomaamisesta

Sormenjälkitunnistus on näkymätöntä, eikä ole helppoa selvittää käyttääkö sivusto sitä (Durey ym. 2021). Al-Fannah, Li ja Mitchell (2018) mukaan mikään suurimmasta neljästä selaimesta, joita käyttää 88 % kaikista internetin käyttäjistä, ei varoita käyttäjää, jos sivusto esittää sormenjälkitunnistukselle tyypillisiä merkkejä. Nykyään kuitenkin Firefox esittää pienen kilven muotoisen symbolin selaimen osoitepalkissa, jos se huomaa ja estää seuraimia sivustolla. Firefoxin mukaan sormenjälkitunnistus kuuluu estettyihin seuraimiin (Firefox 2021).

Joistain sormenjälkitunnistustekniikoista ei jää minkäänlaista jälkeä. Esimerkiksi passiiviset tekniikat eivät jätä jälkiä ollenkaan (Al-Fannah ja Mitchell 2020). Aktiivinen sormenjälkitunnistus on myös vaikeaa huomata, mutta siihen löytyy joitain tapoja (Englehardt ja Narayanan 2016).

Yksi tapa huomata sormenjälkitunnistus on tarkastella sivuston JavaScript-koodia (Englehardt ja Narayanan 2016). JavaScriptiäkin tutkimalla sormenjälkitunnistuksen huomaaminen on kuitenkin vaikeaa. Sekä sormenjälkitunnistustekniikat että verkkosivut muuttuvat ja elävät koko ajan, joten on vaikea tunnistaa sormenjälkitunnistusta varten kirjoitetut JavaScriptkoodit (Durey ym. 2021).

Sormenjälkitunnistuksen huomaamisen kehittämiseen on tehty monia tutkimuksia ja sormenjälkitunnistuksesta varoittavia laajennuksia selaimeen on kehitetty. On kuitenkin todettu, että yksikään näistä laajennuksista ei todennäköisesti huomaa kaikkea sormenjälkitunnistusta (Al-Fannah ja Mitchell 2020). Jotkin lisäosat pitävät listaa tunnetuista sormenjälkitunnistukseen käytetyistä JavaScript-koodeista, mutta listojen pitäminen ajan tasalla on haastavaa tekniikoiden muuttumisen ja uudistumisen takia (Kaur ym. 2017). Kaikkia sormenjälkitunnistukseen käytettäviä JavaScript-koodeja ei myöskään tunneta (Iqbal, Englehardt ja Shafiq 2020).

Fingerprint alert-laajennus toimii eri tavalla, kuin muut tutkitut laajennukset, se tutkii JavaScriptin sijaan selaimen ja palvelimen välistä datansiirtoa (Al-Fannah, Li ja Mitchell

2018). Laajennus tutkii sisältääkö kyseinen datansiirto jonkun 17 tunnetusti sormenjälkitunnistukseen käytetyistä attribuuteista ja varoittaa käyttäjää löydöstä (Al-Fannah, Li ja Mitchell 2018). Al-Fannah, Li ja Mitchell (2018) kehittivät laajennuksen oman tutkimuksensa yhteydessä sormenjälkitunnistuksen yleisyydestä.

Tekoälyn valjastamista sormenjälkitunnistuksen tunnistamiseen on myös ehdotettu (Iqbal, Englehardt ja Shafiq 2020). Iqbal, Englehardt ja Shafiq (2020) ehdottavat yhtä tällaista tunnistusmallia. Heidän mallinsa pyrkii tekoälyn avulla tunnistamaan jo entuudestaan tuntemattomia sormenjälkitunnistukseen käytettäviä JavaScript-koodeja jo tunnettujen koodien tutkimisen rinnalla (Iqbal, Englehardt ja Shafiq 2020). Mallin mukaan toteutettu ohjelma pystyi tunnistamaan sormenjälkitunnistuksen 26 % paremmin kuin pelkästään tunnettuja sormenjälkitunnistuskoodeja tarkastelevat laajennukset (Iqbal, Englehardt ja Shafiq 2020).

4 Sormenjälkitunnistuksen toimivuudesta

Tässä tutkimuksessa sormenjälkitunnistuksen toimivuudella tarkoitetaan sitä, kuinka suurelle osalle käyttäjistä saadaan luotua yksilöllinen sormenjälki. Mitä toimivampaa tai korkeampaa toimivuus on, sitä suurempi osa käyttäjistä on saatu yksilöityä sormenjälkitunnistuksella. Tämä käsite määriteltiin ja otettiin käyttöön aiheen selventämiseksi.

Sormenjälkitunnistuksesta ja sen toimivuudesta on tehty monta tutkimusta. Jo ensimmäisissä tutkimuksissa melkein kaikille käyttäjille on saatu luotua yksilöllinen sormenjälki (Mayer 2009; Eckersley 2010). Näiden jälkeen on tehty muutamia suurempia laajamittaisia tutkimuksia erilaisia sormenjälkitunnistustekniikoita käyttäen.

Gómez-Boix, Laperdrix ja Baudry (2018) argumentoivat, että aiemmat tutkimukset, kuten Panopticlick ja AmIUnique, ovat olleet vääristyneitä. Heidän mukaansa tutkimukset on tehty mahdollisesti tietoturvasta kiinnostuneiden ihmisten laitteille, joka vääristää tuloksia (Gómez-Boix, Laperdrix ja Baudry 2018). Tutkijoiden mielestä nämä aiemmat tutkimukset ovat olleet rajoittuneita, eivätkä vastaa internetin todellista väestöä (Gómez-Boix, Laperdrix ja Baudry 2018). Aiempien tutkimusten korkeammat toimivuudet voivat johtua siitä, että tietoturvasta kiinnostuneemmat ihmiset todennäköisemmin pyrkivät suojaamaan laitettaan erilaisilla laajennuksilla, joka lisää sormenjälkitunnistuksen toimivuutta. Gómez-Boix, Laperdrix ja Baudry (2018) suorittivat oman tutkimuksensa yhdellä Ranskan 15 suosituimmista verkkosivuista ja onnistuivat itse luomaan yksilöllisen sormenjäljen 33,6 % käyttäjistä. Heidän mielestään sormenjälkitunnistus ei ole välttämättä niin toimivaa suurilla ihmismäärillä, ja tutkimuksen kohdejoukolla on iso vaikutus sormenjälkitunnistuksen toimivuuteen (Gómez-Boix, Laperdrix ja Baudry 2018).

Toinen tutkimus, joka tehtiin yhteistyössä edellä mainitun tutkimuksen tutkijoiden kanssa, raportoi hyvin erilaisia tuloksia. Molemmilla tutkimuksilla oli sama kerätty data, mutta Gómez-Boix, Laperdrix ja Baudry (2018) tekivät tutkimuksensa käyttäjien seurannan näkökulmasta ja tarkastelivat 17 attribuuttia, kun taas Andriamilanto, Allard ja Guelvouit (2021) ottivat näkökulmakseen käyttäjien todentamisen sormenjälkitunnistusta

hyödyntäen ja tarkastelivat 216 attribuuttia. Andriamilanto, Allard ja Guelvouit (2021) onnistuivat yksilöimään 81,8 % käyttäjistä. He myös todistivat yksilöllisten sormenjälkien olevan stabiileja, eli yksilöllinen sormenjälki todennäköisesti pysyy yksilöllisenä (Andriamilanto, Allard ja Guelvouit 2021).

Sormenjälkitunnistuksen toimivuudesta kaivattaisiin lisää laajamittaisia tutkimuksia erilaisilla kohdeyleisöillä. Olisi erittäin tärkeää pyrkiä toistamaan Gómez-Boix, Laperdrix ja Baudry (2018) tutkimus globaalimmalla väestöllä, tai tehdä enemmän heidän tutkimukseensa verrattavia tutkimuksia. Ilman näitä on vaikeaa saada kunnollista kokonaiskuvaa sormenjälkitutkimuksen toimivuudesta reaalimaailmassa.

Sormenjälkitunnistukseen kehitetään koko ajan uusia entistä tehokkaampia tekniikoita (Englehardt ja Narayanan 2016). Näin ollen sormenjälkitunnistuksen toimivuuden voi siis olettaa nousevan koko ajan.

Sormenjälkitunnistuksen toimivuuteen liittyy se, miksi se on niin vaikeaa estää. Koska sormenjälkitunnistus on mahdollista toteuttaa niin monella eri tavalla, on vaikeaa estää kaikki sormenjälkitunnistus (Al-Fannah ja Mitchell 2020). Se, että monet sormenjälkitunnistuksen vastaiset tekniikat tekevät sormenjälkitunnistuksesta vain entistä toimivampaa (Al-Fannah ja Mitchell 2020), kertoo myös sormenjälkitunnistuksen toimivuudesta.

5 Miksi sormenjälkitunnistus on uhka yksityisyydelle

Sormenjälkitunnistusta pidetään yleisesti riskinä käyttäjien yksityisyydelle. Tässä luvussa esitellään sormenjälkitunnistuksen piirteitä, jotka ovat uhkia, tai voivat luoda uhkia käyttäjän yksityisyydelle.

Sormenjälkitunnistuksesta suuremman uhan muihin seurausteknikoihin, kuten evästeisiin, verrattuna tekee sen näkymättömyys. Nykyään verkkosivujen tarvitsee erikseen kysyä käyttäjiltä suostumusta evästeiden käyttöön ja 1/3 käyttäjistä poistaa evästeet säännöllisesti (Nikiforakis ym. 2013). Sormenjälkitunnistus ei jätä näkyviä jälkiä toiminnastaan (Al-Fannah ja Mitchell 2020), eikä se kysy käyttäjän suostumusta tietojen

keräämiseen (Acar ym. 2013; Durey ym. 2021). Lisäksi on erittäin vaikea selvittää käyttääkö sivu sormenjälkitunnistusta, kuten tässä tutkimuksessa on aiemmin esitetty luvussa 3. Sormenjälkitunnistus ei säilytä mitään tietoa käyttäjän puolella (Adamsky, Schiffner ja Engel 2020), joten käyttäjä ei itse voi poistaa sen keräämiä tietoja (Kaur ym. 2017). Sormenjälkitunnus ja sillä kerätyt tiedot ovat siis käytännössä pysyviä (Al-Fannah, Li ja Mitchell 2018). Käyttäjä ei siis pysty itse tarkastelemaan mitä tietoa hänestä on kerätty, eikä vaikuttamaan ollenkaan kerättyjen tietojen sisältöön tai olemassaoloon.

Sormenjälkitunnistusta voi käyttää myös evästeiden toiminnan muuttamiseksi. Koska sormenjälkitunnistus tunnistaa käyttäjän evästeistä huolimatta, voi sitä käyttää poistettujen evästeiden palauttamiseen (Kaur ym. 2017). Nämä ovat niin sanottuja supercookieita (AlFannah ja Mitchell 2020).

Sormenjälkitunnistuksen estäminen on käyttäjälle vaikeaa, eikä siihen toimi samat keinot kuin evästeisiin. Sormenjälkitunnistusta ei voi estää esimerkiksi käyttämällä yksityistä selainta (Acar ym. 2013), vaan se vaatii järeämmät keinot seurauksen estämiseksi. Yksityisen selaimen käyttö ei estä sormenjälkitunnistusta, sillä sormenjälkitunnistus voi olla laitekohtainen selaimesta riippumaton sormenjälki. Sormenjälkitunnistuksen estämistä käsitellään tarkemmin seuraavassa luvussa (luku 6).

Sormenjälkitunnistuksessa pystyy käyttämään lähes mitä tahansa tietoa käyttäjän laitteesta
(Al-Fannah ja Mitchell 2020). Li ja Cao (2020) huomasivat tutkimuksessaan, että sormenjälkitunnistusteknologioita hyödyntäen pääsi käsiksi laitteen hymiöihin. Tietoa siitä, mitä hymiöitä laitteella on, voisi käyttää sormenjälkitunnistuksessa, tai selvittämään onko laitteelle tehty tietoturvapäivityksiä (Li ja Cao 2020). He esittelevät tutkimuksessaan useamman esimerkin tilanteesta, jossa samassa päivityksessä on tullut korjauksia laitteen tietoturvaan ja päivityksiä emojeihin.

Al-Fannah, Li ja Mitchell (2018) huomasivat tutkimuksessaan, jossa tarkasteltiin sivustojen ja selaimen välistä dataa, että kaikki sivustot eivät käyttäneet HTTPS-yhteyttä käyttäjän sormenjälkitietojen tiedonsiirrossa. HTTPS-yhteys on HTTP-yhteyden tietoturvallisempi

muoto. Siinä siirretty tieto salataan ensin. Heidän mukaansa 50 % sivustoista käytti salaamatonta HTTP-yhteyttä henkilöiden tunnistukseen käytettävän tiedon siirtoon. Al-Fannah, Li ja Mitchell (2018) toteavat myös, että jotkin verkkosivut laittoivat selaimen palauttamaan arvon, joka oli selkeästi nimetty sormenjäljeksi ja sisälsi sormenjälkitunnistukseen käytettävää tietoa. Heidän mukaansa tätä sormenjälkiarvoa vaikutettaisiin käytettävän käyttäjien tunnistukseen ja jotkut sivustot jakoivat näitä arvoja keskenään. Sormenjälkitunnusten jakaminen tahojen kesken lisää sormenjälkitunnistuksen uhkaa käyttäjien yksityisyydelle (Al-Fannah,
Li ja Mitchell 2018)

Verkkosivun ylläpitäjät eivät usein edes ole tietoisia, että joku kolmas osapuoli käyttää heidän sivustoaan sormenjälkitunnistukseen ja tietojen keräämiseen (Englehardt ja Narayanan 2016). Monet sivustot ostavat JavaScript-koodinsa kolmannelta osapuolelta, eivätkä siis itse mahdollisesti ole täysin tietoisia kaikesta sen sisällöstä (Al-Fannah, Li ja Mitchell 2018). Tämä lisää sormenjälkitunnistuksen yksityisyyden uhkaa, sillä tällaisissa tapauksissa ei ole selkeää kenelle käyttäjän tiedot menevät.

6 Sormenjälkitunnistusta vastaan suojautuminen

Monet eri tutkimukset ovat arvioineet erilaisia suojautumiskeinoja ja esitelleet omia ehdotuksiaan sormenjälkitunnistusta vastaan. Tässä luvussa käsitellään yleisimpiä suojauskeinoja sormenjälkitunnistusta vastaan, sekä niiden toimivuutta.

6.1 Yleistä suojautumisesta

Sormenjälkitunnistukselta suojautuminen on todella haastavaa, ellei jopa mahdotonta. Sormenjälkitunnistus pystyy hakemaan samat tiedot käyttäjästä monella tapaa, joten kun yksi tapa estetään, saadaan samat tiedot silti haettua (Nikiforakis ym. 2013). Eston vaikeutta lisää sormenjälkitunnistuksen näkymättömyys. Ei tiedetä mitkä sivustot tarkalleen käyttävät tunnistusta, eikä tiedetä, onko kaikessa tunnistuksen estämisessä onnistuttu (Al-Fannah ja Mitchell 2020).

Joitain sormenjälkitunnistuksia voidaan estää ottamalla JavaScript pois päältä, mutta se tekee internetin käyttämisestä todella epämukavaa. Kuten aiemmin mainittu, lähes kaikki verkkosivustot käyttävät JavaScriptia ja sen estäminen täysin rikkoisi siis lähes kaikki verkkosivut. Lisäksi koska vain 1 % internetin käyttäjistä estää JavaScriptin (Kaur ym. 2017), tulee sormenjäljestä todennäköisesti silti yksilöllinen. JavaScriptin estämistä voidaan käyttää yhtenä osana sormenjälkeä (Kaur ym. 2017).

Jotkin sormenjälkitunnistuksen vastaiset tekniikat pyrkivät muuttamaan käyttäjän tietoja ja näin huijata sormenjälkitunnistusta. Tämä tekniikka kohtaa saman ongelman kuin edellä mainittu. Kun samat tiedot pystytään hakemaan montaa eri tekniikkaa hyödyntäen, on vaikeaa saada kaikki muutettua (Nikiforakis ym. 2013). Sormenjälkitunnistus on voitu myös tehdä sellaiseksi, että jos se huomaa jonkun attribuutin arvon olevan mahdoton (Nikiforakis ym. 2013), tai erilainen kahdella tapaa haettua, se tietää että tietoja väärennetään ja lisää sormenjälkeen muuttujaksi suojautumisyrityksen (Kaur ym. 2017). Tämä vain lisää sormenjälkitunnistuksen toimivuutta.

Tätä edellä mainittua sormenjälkitunnistuksen ominaisuutta, jossa tunnistetaan suojautumisyritys, kutsutaan englanniksi termeillä detection of defence tai fingerprintability paradox (Al-Fannah ja Mitchell 2020). Näillä termeillä tarkoitetaan sitä, että sormenjälkitunnistukselta suojautuminen tekee sormenjälkitunnistuksesta aiempaa helpompaa (Al-Fannah ja Mitchell 2020). Monet sormenjälkitunnistukselta suojautumismenetelmät kaatuvat tähän samaan ongelmaan.

Jotkin selaimet, kuten Mozilla Firefox, ovat ottaneet kokeiluun erilaisia sormenjälkitunnistusta estäviä toimenpiteitä (Bird ym. 2020; Firefox 2021). Al-Fannah ja Mitchell (2020) mukaan suurimpien selaimien pitäisi ottaa askeleita sormenjälkitunnistuksen estämiseksi, sillä se olisi ainoa tapa saada estettyä sormenjälkitunnistus tehokkaasti. Sormenjälkitunnistuksen estäminen on käyttäjälle työlästä ja haittaa käyttäjän kokemusta selata verkkoa, joten selaimien työ tämän eteen olisi erityisen tärkeää.

6.2 Laajennukset

Tällä hetkellä selaimiin on saatavilla monenlaisia yksityisyyttä suojaavia laajennuksia. Osa näistä laajennuksista lupaa suojausta sormenjälkitunnistusta vastaan. Laajennuksilla on samat heikkoudet sormenjälkitunnistuksen estämisessä, kuin mikä niillä on sormenjälkitunnistuksen huomaamisessakin.

Sormenjälkitunnistukselta suojaavat laajennukset voidaan jakaa kahteen alakategoriaan: Sormenjälkiarvoja väärentävät laajennukset ja JavaScript-koodien toiminnan estävät laajennukset(Bird ym. 2020). Sormenjälkiarvoja väärentävät laajennukset törmäävät aiemmin esitettyihin ongelmiin. Yksi laajennus ei pysty väärentämään tiettyä arvoa kaikilla tavoilla, joilla arvo on mahdollista noutaa (Kaur ym. 2017).

JavaScriptia estävien laajennuksien tarkoituksena on estää vain tietyt JavaScript-koodit, jolloin käyttäjän ei tarvitse ottaa JavaScriptia kokonaan pois päältä. Nämä laajennukset usein hyödyntävät listoja estettävistä koodeista. Nämä listat ovat usein vajavaisia, sillä listojen ylläpito on työlästä (Bird ym. 2020). Mitkään laajennukset eivät myöskään kykene huomaamaan kaikkea sormenjälkitunnistusta ja estävät usein vahingossa verkkosivun toimintaan käytettyä koodia rikkoen sivuston (Al-Fannah, Li ja Mitchell 2018).

Laajennuksista huonon vaihtoehdon sormenjälkitunnistuksen estämiseen tekee se, että selaimelle ladattuja laajennuksia voidaan käyttää yhtenä osana sormenjälkitunnuksen luomisessa (Kaur ym. 2017). Kuten aiemmin esitetty, mitä enemmän sormenjälkitunnistukselta suojaavia laajennuksia käyttäjä lataa, sitä uniikimpi sormenjälki hänellä on. Ei myöskään ole keinoa selvittää onnistuvatko laajennukset oikeasti estämään sormenjälkitunnistuksen, sillä sormenjälkitunnistus on näkymätöntä (Durey ym. 2021).

6.3 Tor-selain

Tor-selain on Firefox-selaimesta muokattu versio, jonka tavoitteena on estää sivustojen välinen sormenjälkitunnistus (Kaur ym. 2017). Tor-selain toimii muokkaamalla käyttäjän tiedot kaikille käyttäjille mahdollisimman samanlaisiksi (Iqbal, Englehardt ja Shafiq 2020).

Torselain muuttaa muun muassa user-agent tietueen kaikille käyttäjille samaksi (Kaur ym. 2017).

Tor-selain estää sormenjälkitunnistusta myös rajoittamalla verkkosivujen ominaisuuksia, ellei näille erikseen anneta lupaa käyttää estettyjä ominaisuuksia (Li ja Cao 2020). Esimerkiksi Tor-selain estää JavaScriptin käytön kokonaan. Tor-selain myös rajoittaa sallittujen fonttien määrää (Acar ym. 2013), jolloin laitteelle ladattuja fontteja ei voi käyttää sormenjälkitunnistukseen.

Tor-selain tarjoaa vahvan suojan sormenjälkitunnistusta vastaan, jopa joka 58. sormenjälki on identtinen Tor-selaimella (Kaur ym. 2017) Sen heikkoudeksi tällä hetkellä tulee sen vähäinen käyttäjämäärä (Al-Fannah ja Mitchell 2020). Kun käyttäjiä on vähän, pienikin ero riittää muuttamaan sormenjäljen yksilölliseksi (Acar ym. 2013).

Tor-selaimen toinen heikkous on sen käytön epämukavuus (Laperdrix ym. 2020). Verkkosivujen lataus selaimella saattaa olla hidasta (Al-Fannah ja Mitchell 2020) ja monet verkkosivut se rikkoo kokonaan JavaScriptin estämisen takia (Iqbal, Englehardt ja Shafiq 2020). Selainta ei myöskään saisi laittaa kokonäytön tilaan, sillä näytön kokoa ei voida väärentää (Al-Fannah ja Mitchell 2020). Kaikilla käyttäjillä tulisi siis olla samankokoinen selainikkuna käytössä, jotta näytön koko olisi käyttäjillä sama. Kaur ym. (2017) pitävät Tor-selaimen nousemista suurempaan käyttöön epätodennäköisenä, juuri näiden käyttöepämukavuuksien
takia.

6.4 Brave-selain

Brave on vuonna 2019 julkaistu selain (Brave 2019). Brave on hieman yli vuodessa saavuttanut yli 25 miljoonaa aktiivista käyttäjää (Brave 2021) Se markkinoi itseään nopeimpana, tehokkaimpana ja turvallisimpana selaimena (“Features” 2021). Brave lupaa myös eston sormenjälkitunnistusta vastaan (“Features” 2021).

Brave-selaimen tekniikka estää sormenjälkitunnistusta eroaa Tor-selaimesta huomattavasti. Kun Tor-selain pyrkii muuttamaan käyttäjien tietoja mahdollisimman samanlaisiksi, Pyrkii Brave muuttamaan kaikkien käyttäjien tiedot mahdollisimman

erilaisiksi (“Fingerprinting Protections” 2020). Brave-selaimessa sormenjälkitunnistuksen esto perustuu sormenjäljen jatkuvaan muuttumiseen. Brave-selain tekee sormenjäljestä erilaisen joka verkkosivun avauksella (“Fingerprinting Protections” 2020). Sormenjälkeä ei voida käyttää käyttäjän seuraamiseen tai tunnistamiseen, koska se muuttuu jatkuvasti erilaiseksi (“Fingerprinting Protections” 2020).

Brave-selain on niin uusi, että ei löytynyt tutkimuksia, joissa arvioitaisiin Brave-selaimen tehokkuutta sormenjälkitunnistusta vastaan.

6.5 Muut

Al-Fannah ja Mitchell (2020) ehdottavat sormenjälkitunnistuksen korvaamista lisäämällä selaimiin oma uniikki tunnuksensa. Tämän tunnuksen käyttöä olisi käyttäjän mahdollista itse rajoittaa. Heidän mielestään tämä kannustaisi selaimia tekemään askeleita sormenjälkitunnistuksen estämiseksi. kohdennettu mainonta sillä

Kaur ym. (2017) ehdottavat huolellisesti suunnitellun tietojenväärentämismenetelmän kehittämistä. Menetelmän tulisi toimia verkkosivuja rikkomatta ja olla laajassa käytössä (Kaur ym. 2017). Laaja käyttö estäisi vastaavat ongelmat, kuin mitä Tor-selain kohtaa. He pitävät menetelmän laajaa käyttöönottoa erityisen tärkeänä. Heidän menetelmän tulisi toimia myös ilman, että sormenjälkitunnistus huomaisi huijausyrityksen (Kaur ym. 2017).

Yksi tapa estää sormenjälkitunnistusta on laajennukset, jotka vain varoittavat sormenjälkitunnistuksesta (Al-Fannah ja Mitchell 2020). Kun käyttäjää varoitetaan sormenjälkitunnistukselta vaikuttavasta toiminnasta, käyttäjä voi valita olla käyttämättä verkkosivua. Monella suositulla ja nykyään melkein välttämättömällä verkkosivulla kuitenkin on käytössä sormenjälkitunnistusta, joten tällainen käytöksenmuutos vaikuttaa epätodennäköiseltä.

7 Yhteenveto

Tutkimuksen tarkoituksena oli selvittää seuraavat asiat sormenjälkitunnistukseen liittyen:

- Kuinka moni sivusto käyttää sormenjälkitunnistusta?
- Kuinka hyvin sormenjälkitunnistuksella saadaan yksilöityä käyttäjät?
- Mistä tietää käyttääkö sivusto sormenjälkitunnistusta?
- Onko sormenjälkitunnistuksella seuraamista mahdollista estää?

Tutkimuksessa selvisi, että suosituimmasta 10 000 verkkosivustosta noin 68,8 % käyttää sormenjälkitunnistusta, mukaanluettuna Google ja Facebook.

Kaiken sormenjälkitunnistuksen huomaamiseen ei saatu yksiselitteistä kaiken huomaavaa tapaa, mutta esitettiin muutamia tapoja huomata joitain sormenjälkitunnistustekniikoita. On vaikeaa tietää, huomataanko kaikki sormenjälkitunnistus, sillä se on näkymätöntä, eikä välttämättä jätä ollenkaan jälkiä.

Sormenjälkitunnistusta ei nykyisillä tekniikoilla ole mahdollista estää täysin ilman, että käyttäjäkokemus kärsii huomattavasti. Tosin Brave-selaimen eston tehokkuudesta ei löytynyt vielä tieteellisessä kirjallisuudessa näyttöä. Mikäli Brave-selaimen sormenjälkitunnistuksen esto on tehokasta, ei käyttäjäkokemus enää kärsisi estotoimenpiteistä.

Sormenjälkitunnistuksen toimivuudesta ei löytynyt ristiriidatonta tietoa, mutta tiedetään, että se toimii jollain tasolla ja on käytössä reaalimaailmassa. Monien tutkimusten mukaan sormenjälkitunnistuksen toimivuus on kuitenkin korkeaa.

Tutkimuksen heikkoutena on sen rajoittuneisuus kirjallisuuskatsaukseksi. Tutkielmaa olisi parantunut, jos olisi pystynyt luomaan omaa tutkimusta aiheesta ja näin saatu esitettyä uutta tietoa. Tutkimusta rajoitti myös aiheen tuoreus, kaikista osa-alueista ei ole vielä tehty tarpeeksi tutkimusta selkeän kuvan saamiseksi.

Sormenjälkitunnistuksesta olisi tärkeää tehdä enemmän laajamuotoisia tutkimuksia sen toimivuudesta. Näin saataisiin parempi kuva siitä, kuinka hyvin se oikeasti toimii. Tähän

mennessä tehdyt tutkimukset ovat kaikki omilla tavoillaan rajoittuneita, niin kuin tutkimuksilla on tapana. Ongelmaksi nousee kuitenkin se, että näitä laajempia tutkimuksia ei ole montaa. Jos laajempia tutkimuksia olisi useampia, olisi helpompi päätellä mitkä muuttujat vaikuttavat miten sormenjälkitunnistuksen toimintaan. Nyt on vaikeaa arvioida onko esimerkiksi Gómez-Boix, Laperdrix ja Baudry (2018) mainitsemalla tutkittavalla väestöllä niin suuri vaikutus kun he omassa tutkimuksessaan esittävät.

Lisää tutkimusta tulisi myös tehdä sormenjälkitunnistuksen estoon. Tarvittaisiin tutkimusta uusiin keinoihin estää sormenjälkitunnistusta, sekä lisää tutkimusta olemassa olevien keinojen kehittämiseksi. On selkeää, että sormenjälkitunnistus on uhka käyttäjien yksityisyydelle ja sormenjälkitunnistusta olisi jollain tavoin pystyttävä estämään käyttäjien yksityisyyden suojaamiseksi.

Lähteet

Acar, Gunes, Marc Juarez, Nick Nikiforakis, Claudia Diaz, Seda Gürses, Frank Piessens ja Bart Preneel. 2013. “FPDetective: Dusting the Web for Fingerprinters”, 1129–1140. CCS ’13. Berlin, Germany: Association for Computing Machinery. ISBN: 9781450324779.

Adamsky, Florian, Stefan Schiffner ja Thomas Engel. 2020. “Tracking Without Traces—Fingerprinting in an Era of Individualism and Complexity”. Teoksessa *Annual Privacy Forum,* 201–212. Springer.

Andriamilanto, Nampoina, Tristan Allard ja Gaëtan Le Guelvouit. 2021. ““Guess Who?” Large-Scale Data-Centric Study of the Adequacy of Browser Fingerprints for Web Authentication”. Teoksessa *Innovative Mobile and Internet Services in Ubiquitous Computing,* toimittanut Leonard Barolli, Aneta Poniszewska-Maranda ja Hyunhee Park, 161–172. Cham: Springer International Publishing.

Bird, Sarah, Vikas Mishra, Steven Englehardt, Rob Willoughby, David Zeber, Walter Rudametkin ja Martin Lopatka. 2020. “Actions speak louder than words: Semi-supervised learning for browser fingerprinting detection”. *arXiv preprint arXiv:2003.04463.*

Brave. 2019. *Brave Launches Next-Generation Browser that Puts Users in Charge of Their Internet Experience with Unmatched Privacy and Rewards.* Saatavilla WWW-muodossa, https://brave.com/brave-launches-next-generation-browser/, viitattu 29.4.2021.

----. 2021. *Brave Passes 25 Million Monthly Active Users.* Saatavilla WWW-muodossa, https://brave.com/25m-mau/, viitattu 29.4.2021.

Bujlow, T., V. Carela-Español, J. Solé-Pareta ja P. Barlet-Ros. 2017. “A Survey on Web Tracking: Mechanisms, Implications, and Defenses”. *Proceedings of the IEEE* 105 (8): 1476–1510.

Durey, Antonin, Pierre Laperdrix, Walter Rudametkin ja Romain Rouvoy. 2021. “An iterative technique to identify browser fingerprinting scripts”. *arXiv preprint arXiv:2103.00590.*

Eckersley, Peter. 2010. “How unique is your web browser?” Teoksessa *International Symposium on Privacy Enhancing Technologies Symposium,* 1–18. Springer.

Englehardt, Steven, ja Arvind Narayanan. 2016. “Online tracking: A 1-million-site measurement and analysis”. Teoksessa *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security,* 1388–1401.

Al-Fannah, Nasser Mohammed, Wanpeng Li ja Chris J Mitchell. 2018. “Beyond cookie monster amnesia: Real world persistent online tracking”. Teoksessa *International Conference on Information Security,* 481–501. Springer.

Al-Fannah, Nasser Mohammed, ja Chris Mitchell. 2020. “Too little too late: can we control browser fingerprinting?” *Journal of Intellectual Capital.*

“Features”. 2021. https://brave.com/features/.

“Fingerprinting Protections”. 2020. https://github.com/brave/brave-browser/wiki/Fingerpri nting-Protections.

Firefox. 2021. *Firefox blocks fingerprinting.* Saatavilla WWW-muodossa, https://www.mozilla.org/en-US/firefox/features/block-fingerprinting/, viitattu 29.4.2021.

Gómez-Boix, Alejandro, Pierre Laperdrix ja Benoit Baudry. 2018. “Hiding in the crowd: an analysis of the effectiveness of browser fingerprinting at large scale”. Teoksessa *Proceedings of the 2018 world wide web conference,* 309–318.

Iqbal, Umar, Steven Englehardt ja Zubair Shafiq. 2020. “Fingerprinting the Fingerprinters: Learning to Detect Browser Fingerprinting Behaviors”. *arXiv preprint arXiv:2008.04480.*

K. V. Nair, E. RoseLalson. 2018. “The Unique Id’s you Can’t Delete: Browser Fingerprints”. Teoksessa *2018 International Conference on Emerging Trends and Innovations In Engineering And Technological Research (ICETIETR),* 1–5.

Kaur, N., S. Azam, K. Kannoorpatti, K. C. Yeo ja B. Shanmugam. 2017. “Browser Fingerprinting as user tracking technology”. Teoksessa *2017 11th International Conference on Intelligent Systems and Control (ISCO),* 103–111.

Laperdrix, Pierre, Nataliia Bielova, Benoit Baudry ja Gildas Avoine. 2020. “Browser Fingerprinting: A Survey”. *ACM Trans. Web* (New York, NY, USA) 14, numero 2 (huhtikuu). ISSN: 1559-1131.

Li, Song, ja Yinzhi Cao. 2020. “Who Touched My Browser Fingerprint? A Large-scale Measurement Study and Classification of Fingerprint Dynamics”. Teoksessa *Proceedings of the ACM Internet Measurement Conference,* 370–385.

Mayer, Jonathan R. 2009. “Any person... a pamphleteer”: Internet Anonymity in the Age of Web 2.0”. *Undergraduate Senior Thesis, Princeton University,* 85.

Nikiforakis, N., A. Kapravelos, W. Joosen, C. Kruegel, F. Piessens ja G. Vigna. 2013. “Cookieless Monster: Exploring the Ecosystem of Web-Based Device Fingerprinting”. Teoksessa *2013 IEEE Symposium on Security and Privacy,* 541–555.

Schuh, J. 2013. *Saying Goodbye to Our Old Friend NPAPI.* Saatavilla WWW-muodossa, https://blog.chromium.org/2013/09/saying-goodbye-to-our-old-friend-npapi.html, viitattu 15.2.2021.