Mauno Pasanen

Reunalaskennan tietoturva nykyaikaisessa ajoneuvossa

Tietotekniikan pro gradu -tutkielma

25. syyskuuta 2022

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Mauno Pasanen

Yhteystiedot: mjpasane@jyu.fi

Ohjaaja: Tapio Frantti

Työn nimi: Reunalaskennan tietoturva nykyaikaisessa ajoneuvossa

Title in English: Edge Computing security in modern vehicle

Työ: Pro gradu -tutkielma

Opintosuunta: Teknis-matemaattisen mallintamisen ja päätösanalytiikan opintosuunta

Sivumäärä: 84+4

Tiivistelmä:

Teknologian kehittymisen myötä arkipäiväiset laitteet, kuten kodinkoneet ja ajoneuvot, muuttuvat älykkäiksi esineiden internetin toimijoiksi. Siirrettävänä voi olla tietoja miljardeista laitteista, tai on käsiteltävä tietoa ilman merkittävää viivettä. Perinteisen datakeskusvetoisen pilvilaskennan törmätessä haasteisiin näitä ratkomaan on kehittynyt pilvilaskennan osa-alue reunalaskenta, joka käsitteenä tuo tiedon käsittelyn laitteeseen tai laitteen lähelle. Reunalaskennan laajeneminen on kasvattanut myös reaalimaailman turvallisuusuhkia, ja esimerkkejä miljoonien laitteiden tai yksittäisten ajoneuvojen haltuunotosta on lukuisia. Tietoturvan toteutuneet haasteet vaikuttavat laajasti miljoonien ihmisten elämään, liiketoimintaan ja yhteiskunnan toimivuuteen.

Tutkielmassa kootaan yhteen reunalaskennan tietoturvaan kohdistuvia haasteita ja käsitellään ongelmakohtiin kehitettyjä ratkaisuja keskittyen autoihin reunalaitteina. Moderni auto on monipuolinen reunatoimija, johon kohdistuneiden hyökkäysten määrä on Chattopadhyay, Lam ja Tavva (2021) mukaan yli kuusinkertaistunut viime vuosina. Tutkielmassa tehdään ajoneuvon hyökkäysrajapintojen läpikäynti ja uhka-analyysi. Löydösten perusteella analysoidaan tarkemmin kahden, osittain itseajavan ja verkottuneen, auton etähallintaohjelmisto ja jaettu verkkoyhteys suorittamalla sekä välimieshyökkäys että verkkoskannaus, ja analysoimalla verkkoliikenne. Tuloksista on nähtävissä, että valmistajat ovat huomioineet ilmiselvät

riskit. Analyysissä paljastui kuitenkin haavoittuvaisuuksia ja heikkouksia, joihin tehtiin suosituksia, joilla yksityisyyden suojaa voitaisiin parantaa, hyökkäyslinjoja sulkea ja väärinkäytösten mahdollisuutta pienentää. Autojen ollessa pitkäikäisiä hyödykkeitä, niiden suojauksen pitää kestää sekä nykyiset että tulevaisuuden kehittyneemmät hyökkäystekniikat.

Avainsanat: esineiden internet, IoT, sumulaskenta, reunalaskenta, pilvilaskenta. tietoturva, ajoneuvo, auto, itseajava

Abstract:

With the development of technology, everyday devices, such as home appliances and vehicles, are becoming smart Internet of Things players. The data transfer amount can be large from billions of devices, or data must be processed without significant delay. As traditional data center-driven cloud computing faces challenges, the edge computing has evolved to bring data processing to or near the device. The expansion of edge computing has also increased real-world security threats, with numerous examples of hijacking millions of devices or individual vehicles. The realized challenges of information security have a far-reaching impact on the lives of millions of people, businesses and functioning of society.

This thesis brings together the challenges of edge computing security and addresses the solutions developed to the problem areas, focusing on cars as edge devices. The modern car is a versatile edge device, and the number of attacks against them have grown over sixfold in recent years according the Chattopadhyay, Lam ja Tavva (2021). Thesis reviews the vehicle's attack interfaces and performs a threat analysis. Based on the findings, the remote management software and shared network connection of the two self-driven and connected cars are analyzed in more detail by performing a man-in-the-middle attack and a network scan, and analyzing the network traffic. The results show that the manufacturers have taken into account the obvious risks. However, the analysis revealed vulnerabilities and weaknesses, which could be closed, privacy protection could be improved and potential for abuse significantly reduced with the thesis recommendations. As cars are long-lived commodities, their protection must withstand both current and future's more advanced attack technologies.

Keywords: Internet of Things, IoT, fog computing, edge computing, cloud computing, security, vehicle, car, self-driving

Esipuhe

Kanditutkielmassani perehdyin sumulaskennan hyödyntämiseen esineiden internetissä. Lähes 30 vuoden työelämän kokemuksella jäin miettimään aihepiirin ongelmia, ja erityisesti tietoturvaa, joka kanditutkielman kirjallisuudessa käytännössä sivuutettiin kokonaan. Reunalaskennan ollessa laajasti käytössä, esimerkiksi älykkäissä kodinkoneissa, terveyslaitteissa, itseajavissa autoissa ja älykaupunkien infrastruktuurissa, aiheeseen liittyi sekä henkilökohtainen että työperäinen kiinnostus. Tutkielman aiheeksi valikoitui reunalaskennan tietoturva, ja tutkimusprosessin aikana se tarkentui nykyaikaisten ajoneuvojen toimintaan reunalaitteina ja niiden kohtaamiin haasteisiin.

Kiitän tässä yhteydessä ohjaajaani Tapio Franttia erinomaisesta sparrauksesta. Perhettä kestämisestä ja tukemisesta.

Kangasalla 25. syyskuuta 2022

Manu

Kuviot

Taulukot

Sisällys

1 Johdanto

Esineiden internet on kasvanut viime vuosina merkittävästi teknologian ja verkkopalvelujen kehittymisen myötä. Valmistajien pyrkiessä kasvattamaan liiketoimintaa, olemassa olevia tiedon keräämisen, tallentamisen ja käsittelyn teknologioita liitetään yhä enemmän jokapäiväisiin laitteisiin, joita ei alun perin suunniteltu näitä varten. Laitteet, kuten kodinkoneet ja ajoneuvot, muuttuvat älykkäiksi esineiden internetin toimijoiksi. Huawei (2018, p.6) ennustaa teknologiavisiossaan vuonna 2025 maailmassa olevan 40 miljardia älylaitetta, joiden välillä olisi 100 miljardia yhteyttä. Cisco (2020) mukaan esineiden internetin laitteiden määrä kasvaa nopeammin (10 % vuotuinen kasvu) kuin maapallon väestö (1 %) tai internetin käyttäjät (6 %), ja ylittävän vuoteen 2023 mennessä 29 miljardin laitteen rajan.

Samalla esineiden internet on kehittymässä yhä enemmän suuntaan, jossa siirrettävänä on suuria tietomassoja miljardeista laitteista, tai on käsiteltävä tietoa ilman merkittävää viivettä. Perinteinen datakeskusvetoinen pilvilaskenta törmää tällöin haasteisiin, joita ratkomaan on syntynyt pilvilaskennan osa-alue reunalaskenta. Käsitteenä reunalaskenta tuo tiedon käsittelyn laitteeseen tai laitteen lähelle. Cisco Global Cloud Indexin arvion mukaan kolmannes maailman dataliikenteestä vuonna 2020 oli esineiden internetin, ihmisten ja esineiden tuottamaa. Tästä reunalla tuotetusta tiedosta 40 % analysoitiin, käsiteltiin ja tallennettiin verkon reunalla (Zhang ym. 2018). Reunalaskennan markkinan arvioitiin kasvavan vuoteen 2026 vuotuisesti yli 29 % noin 11 miljardiin dollariin (ReportLinker 2021).

Reunalaskennan laajeneminen, teknologialupaus ja ainutlaatuiset ominaisuudet, kuten ympäristötietoisuus, reaaliaikainen laskenta ja rinnakkaiskäsittely, ovat kuitenkin tuoneet myös useita uusia haasteita tietoturvan ja yksityisyyden säilyttämisessä. Uhkien suuruusluokasta antaa kuvan Mirai-botnet, jossa hyökkääjä otti 20 tunnin sisällä haltuunsa yli 65 000 esineiden internetin laitetta, kokonaismäärän noustessa myöhemmin 378 miljoonaan laitteeseen. Haltuunotettuja laitteita käytettiin hyväksi palvelunestohyökkäyksessä korkean profiilin reunapalveluntarjoajia kohtaan. (Xiao ym. (2019)). Turvauhkat vaikuttavat konkreettisesti jo nyt suureen osaan maailman ihmisistä ja liiketoiminnasta. Lappeenrannan palvelunestohyökkäys talvella 2016 kaatoi kahden asuinkorttelin lämmitysjärjestelmän jättäen asukkaansa ilman lämmitystä yli viikoksi. Tunnettujen valmistajien autoja, kodinvalvontalaitteita ja leluja, se-

kä niiden sisältämiä tietoja on kaapattu ja hyväksikäytetty. (Euroopan unionin verkko- ja tietoturvavirasto (2017b).)

Muun muassa ihmisten mukavuudenhalun ja kiristyvien turvallisuusvaatimusten, kuten Euro NCAP, European New Car Assessment Programme (2022), takia valmistajat lisäävät reunalaskentakyvykkyyksiä autoihin mahdollistaakseen ajoneuvojen autonomiaa, kuten itseajavuutta. Puoli- ja täysin autonomisten ajoneuvojen markkinoiden ennustetaan olevan kasvussa, ja pelkästään Kiinassa on arvioitu olevan autonomisia autoja vuoteen 2035 mennessä noin 8,6 miljoonaa. Boston Consulting Group arvioi autonomisten ajoneuvojen saavuttavan 25 prosentin markkinaosuuden maailmanlaajuisesti vuosina 2035–2040. (West (2016).) Auto tulee Cisco (2020) mukaan olemaan nopeimmin kasvava esineiden internetin sovellustyyppi. Samalla auton mahdollistamat tiedonkeräysominaisuudet muun muassa teiden kunnosta, säätilasta, liikennetilanteesta tai käyttäjien toimista lisääntyvät ja mahdollistavat valmistajille uudenlaista liiketoimintaa ja -malleja. Nykyiset autot eivät vielä täytä SAE International (2021) määritelmää tason 5 täysin automaattisesta ajamisesta, mutta kykenevät suorittamaan auton hallintaan liittyviä itsenäisiä toimenpiteitä, vaikka vastuu onkin kuljettajalla. Chattopadhyay, Lam ja Tavva (2021) mukaan autoihin kohdistuneiden kyberhyökkäysten määrä on 6-kertaistunut vuodesta 2010 vuoteen 2018. Hyökkäyksissä auto on kyetty esimerkiksi ottamaan viihdejärjestelmää hyödyntäen täysin etähallintaan, tai aiheuttamaan sille onnettomuus häiritsemällä sen valotutkaa. Autot ovat pitkän aikavälin hyödykkeitä, ja on muistettava, että nykyisten modernien autojen sensori-, laskenta-, suojaus- ja salaustekniikat ovat vähemmän tehokkaita tulevaisuudessa.

Tutkielman tavoitteena on viimeisimmän tieteellisen kirjallisuuden pohjalta löytää ja koota yhteen reunalaskennan tietoturvaan kohdistuvia haasteita, käsitellä ongelmakohtiin kehitettyjä ratkaisuja, tarkastella modernia autoa reunalaskentatoimijana erityisesti tietoturvan osalta, löytää mahdollisia avoimia tutkimusalueita, ja konstruktiivisella tutkimusmenetelmällä tehdä ratkaisumalleja ja suosituksia, joilla erityisesti autojen reunalaskennan tietoturvaa voidaan parantaa. Kirjallisuuskatsausta tehtäessä huomattiin suomenkielisen lähdekirjallisuuden vähäisyys, eikä vastaavaa suomenkielistä katsausta myöskään oltu tehty.

Tutkimuskysymykseksi muotoutui

- **Miten modernin ajoneuvon reunalaskennan tietoturvaa voidaan parantaa.**

Tutkielman teoriaosuus toteutettiin kirjallisuuskatsauksena perustuen pääasiassa tieteellisiin julkaisuihin ja standardeihin. Keräämisessä hyödynnettiin pääasiallisena hakukoneena Google Scholaria ja verkossa sijaitsevia sähköisiä tietokantoja ja kirjastoja, kuten JYKDOC, IEEE Xplore Digital Library ja AIS Electronic Library. Lähdeaineiston hakusanoina käytettiin seuraavia: vehicle, edge computing, IoT, fog computing, sumulaskenta, reunalaskenta, self-driving, car, autonomous sekä näiden yhdistelmiä seuraavien hakusanojen kanssa: security, attack, threat, review, survey ja privacy. Lähdeaineisto pyrittiin rajaamaan laadukkaisiin ja luotettaviin tietojenkäsittelyn julkaisuihin viimeisten 5–7 vuoden ajalta ottaen huomioon lähteen viittausten määrän. Lisäksi taustoittamiseen käytettiin erilaisia turvallisuus- ja markkinatutkimuksia, valmistajien antamia tietoja sekä yritysten tutkimuspapereita.

Tutkielma koostuu johdannosta, neljästä sisältöluvusta ja yhteenvedosta. Luvussa 2 käsitellään reunalaskenta esittelemällä sen määritelmiä, toimintaympäristö, ratkaisuja ja niiden tuottamia haasteita tietoturvalle. Luvussa 3 läpikäydään reunalaskennan turvallisuushaasteita ja esimerkkejä hyökkäys- ja hyödyntämistamahdollisuuksista. Haasteisiin ehdotettuja tietoturvaratkaisuja käsitellään luvussa 4. Luvussa 5 tarkastellaan autoa reunalaitteena, tehdään sille yleinen riskikartoitus ja syvennytään esimerkkiautojen tarjoamiin hyökkäysrajapintoihin. Pohdinnassa läpikäydään löydöksistä havainnoituja mahdollisia avoimia tutkimusalueita, ja tehdään ratkaisumalleja ja suosituksia tietoturvan toteuttamiseen. Yhteenvedossa tiivistetään tutkimuskysymykseen löydetyt vastaukset.

2 Reunalaskenta

Reunalaskenta on pilvilaskennan osa-alue, ja kattokäsite, joka kattaa laskentaresurssien tuonnin päätelaitteiden lähelle. Sen taustalla ovat esineiden internetin laaja käyttöönotto ja päätelaitteiden monipuolistuminen. Laitteita, jotka tutkimusten perusteella ovat yleensä resurssirajoitteisia, on täydennettävä laskennallisesti, ja vanha pilvilaskennan malli tarvitsee vaihtoehtoja (Baktir, Ozgovde ja Ersoy 2017). On syytä mainita Yousefpour ym. (2019) tutkimuksen perusteella, että käsitteinä reunalaskentaa, reunapilveä/reunapilvipalvelimia (cloudlets), sumulaskentaa ja usvalaskentaa käytetään joissakin yhteyksissä vaihtokelpoisesti, koska niillä kaikilla ”reuna” toimii yleisenä terminä. Tietoliikennealalla käytetty termi reuna viittaa tavallisesti 4G/5G-tukiasemiin, RAN:iin (Radio Access Network) ja ISP:n (Internet Service Provider) pääsy- tai reunaverkkoihin. Esineiden internetin ympäristössä termi reuna kuitenkin viittaa paikalliseen verkkoon, jossa sensorit ja laitteet sijaitsevat. Toisin sanoen reuna on ensimmäinen välitön verkkohyppy itse laitteista, tarkoittaen esimerkiksi WiFi-tukiasemia tai yhdyskäytäviä. Jos laskenta taas suoritetaan itse esineiden internetin laitteilla, niin tätä laskentamallia kutsutaan usvalaskennaksi. Tutkimuksen mukaan General Electric huomauttaa, että sumulaskenta keskittyy reunalaitteiden (esimerkiksi mobiiliverkon tukiasemat tai reunareitittimet) väliseen vuorovaikutukseen, kun taas reunalaskenta keskittyy yhdistettyihin asioihin liitettyyn tekniikkaan (esimerkiksi WiFi-tukiasemat). (Yousefpour ym. (2019).)

Tutkimuksessaan Baktir, Ozgovde ja Ersoy (2017) ovat analysoineet eri reunalaskentaehdotusten ominaisuuksia, ja todenneet pilvi- ja reunalaskentatekniikoiden välillä seuraavat erot:

Taulukko: Pilvi- ja reunalaskennan vertailua
(Baktir, Ozgovde ja Ersoy (2017) mukaillen)

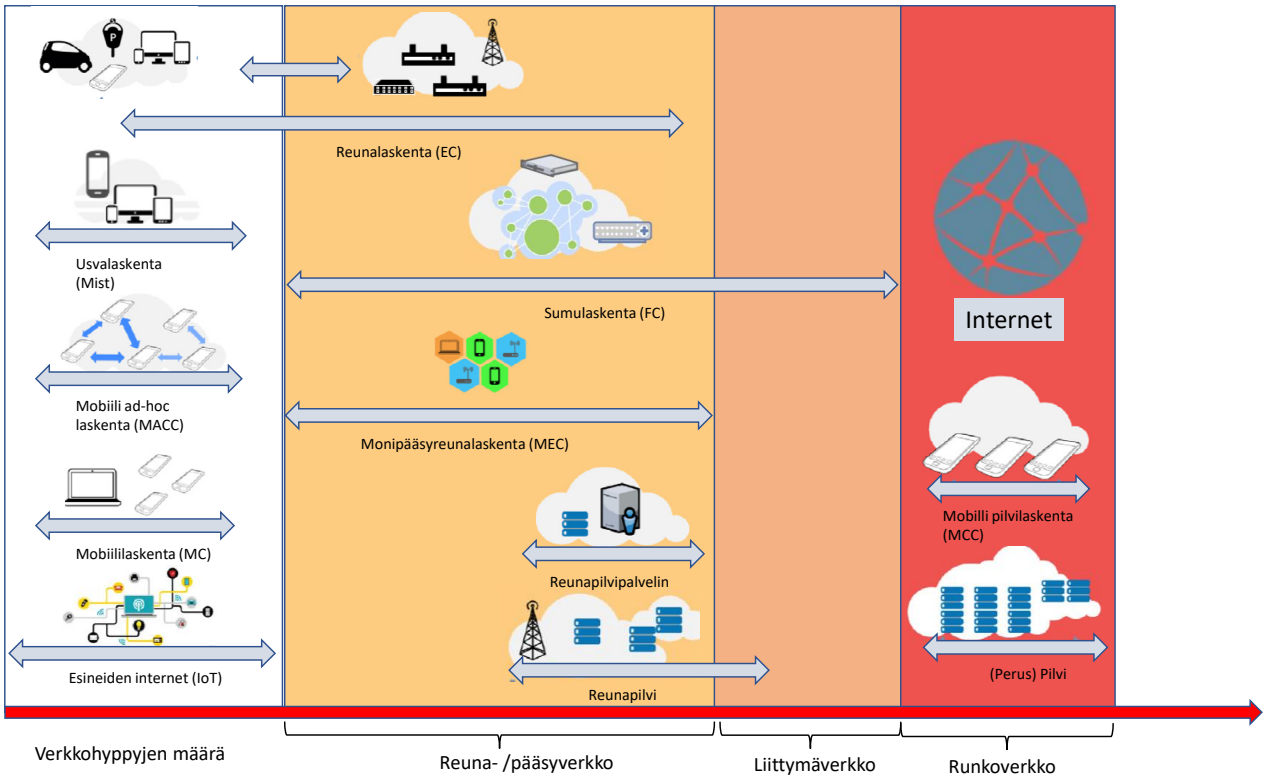
Vaatimukset/ ominaisuudet	Pilvilaskenta	Reunalaskenta
Viive	Korkea	Matala
Verkko	Enimmäkseen laajaverkko (WAN)	Paikallisverkko LAN(WLAN)
Palvelimen sijainti	Missä tahansa verkossa	Reunalla
Liikkuvuuden tuki	Matala	Korkea
Jakautuminen	Keskitetty	Hajautettu
Tehtävän vaatimukset	Suuri laskentateho	Matala latenssi
Laitteet	Tietokoneet, mobiililaitteet rajoitetusti	Kytketyt älylaitteet
Hallinta	Kaupallinen palveluntarjoaja	Paikallinen liiketoiminta
Servereiden määrä	Suuri	Pieni
Yhteyden tila	Uudistettava/korvattava (soft) ja pysyvä (hard)	Uudistettava/korvattava

Reunalaskennan järjestelmien toiminnasta ja arkkitehtuurista on olemassa useita ehdotuksia. Tutkimuksessaan Baktir, Ozgovde ja Ersoy (2017) nostavat esille käsitteet mobiilipilvilaskenta (Mobile Cloud Computing, MCC), reunapilvipalvelin (Cloudlet), sumulaskenta (Fog Computing, FC), reunalaskenta (Edge Computing, EC), mobiilireunalaskenta (Mobile-Edge Computing, MEC) ja usvalaskenta (Mist Computing).

Yllämainittujen lisäksi (Firouzi, Farahani ja Marinšek 2021; Naha ym. 2018) listaavat myös käsitteet kastelaskenta (Dew Computing, DC), sumu-kastelaskenta (Fog-Dew Computing, FDC), läpinäkyvä laskenta (Transparent Computing) ja äärimmäinen reuna (Extreme Edge).

Kaikki nämä käsitteet määrittelevät erilaisia käytännön toteutuksia reunalaskennalle. Tarkasteltuna näillä lähestymistavoilla on yhteiset perusteet, mutta ne eroavat toisistaan ja ovat eri-

koistuneet kohdennettuihin käyttötapauksiinsa. Listan tärkeimpien käsitteiden sijoittuminen esineiden internetin toimintaympäristöön esitetään kuviossa 1.



Kuvio 1. Reunalaskennan käsitteistöä (Yousefpour ym. (2019) mukaillen).

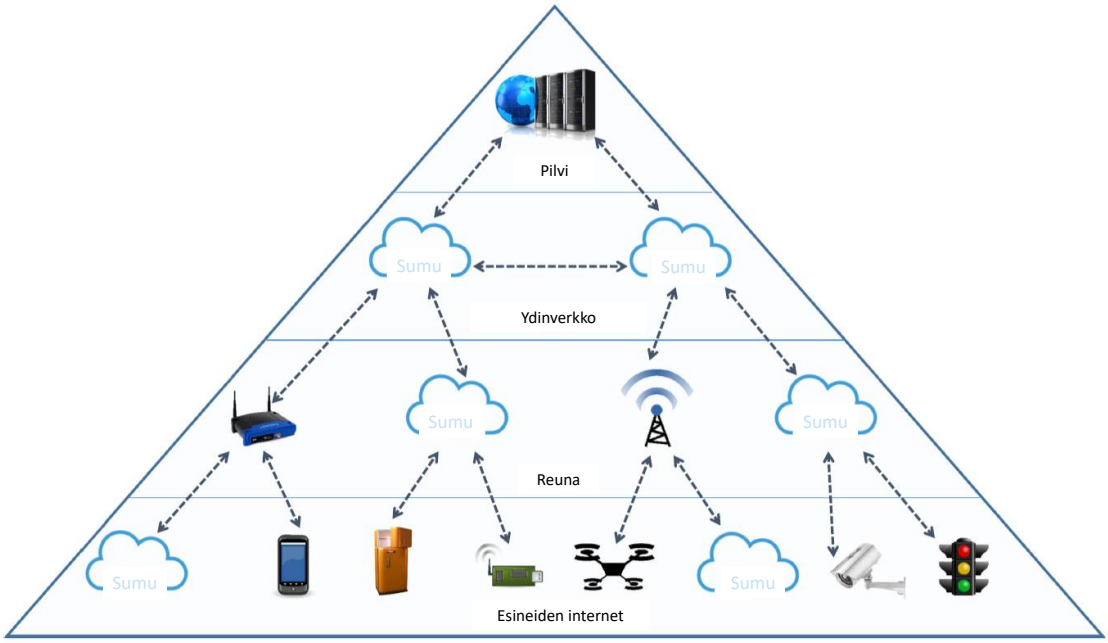
Käsitteistö läpikäydään tarkemmin liitteessä A. Tutkielman kannalta tärkeimmät käsitteet ovat:

- **Reunalaskenta (Edge Computing, EC)** sijaitsee verkon reunalla lähellä esineiden internetin laitteita. Yousefpour ym. (2019) käyttämän määritelmän mukaan reunalaskenta ei ole itse laitteissa, vaan yhden verkkohypyn päässä tapahtuvaa laskentaa. OpenEdge Computing (2021) määrittelee reunalaskennan toiminnaksi, joka suoritetaan verkon laidalla pienissä lähellä käyttäjiä sijaitsevissa datakeskuksissa. NIST määrittää käsitteen päätelaitteet ja niiden käyttäjät kattavaksi verkkokerrokseksi (esineiden internet-verkko), joka tarjoaa paikallisen laskentatoiminnon esimerkiksi sensorissa, mittauslaitteessa tai muissa verkossa käytettävissä laitteissa (Iorga ym. 2018). Esimerkkeinä erilaisesta reunan tulkinnasta Naha ym. (2018) antaa 1) reunapilvipalvelimen sijain-

nin mobiilisovelluksen ja perinteisen pilven välissä, kun taas 2) esineiden internetin yhdyskäytävä on sensorin ja perinteisen pilvipalvelun välinen reuna.

- **Sumulaskenta (Fog Computing, FC)**, on Bonomi ym. (2012), mukaan erittäin virtualisoitu alusta, joka tarjoaa laskenta-, tallennus- ja verkkopalveluja esineiden internetin laitteiden ja perinteisten pilvipalvelutietokeskusten välillä. Sumulaskentaa pidetään useasti synonyyminä reunalaskennalle. Vaikka sumu- ja reunalaskenta siirtävät laskennan ja tallennuksen verkon reunaan ja lähemmäs päätelaitteita, käsitteet eivät ole identtisiä. Yousefpour ym. (2019) mukaan OpenFog konsortio itse asiassa toteaa, että reunalaskentaa kutsutaan usein virheellisesti sumulaskennaksi. OpenFog-konsortio tekee eron siitä, että sumulaskenta on hierarkkinen ja se tarjoaa tietojenkäsittelyn, verkottumisen, tallennuksen, hallinnan ja nopeuttamisen missä tahansa pilvestä esineisiin, kun reunalaskenta taas rajoittuu laskemiseen yhden verkkohypyn päässä laitteista. Sumulaskennan arkkitehtuuria kuvataan hyvin pilveä vastaavaksi, laajentaen pilvipalvelut verkon reunalle. Sumusolmut ottavat käyttöön ja tarjoavat samantyyppisiä XaaS-palveluja kuin pilvipalvelut. Erona pilvilaskentaan sumulaskennan arkkitehtuuri käyttää lisäksi yhtä tai useampaa yhteistyössä toimivaa loppukäyttäjäasiakasta tai läheisen organisaation reunalaitetta, jotka suorittavat huomattavan määrän viestintä-, ohjaus-, määritys-, mittaus- ja hallintapalveluita. (Mahmood (2018, 5).) Arkkitehtuurimallia selventää Puliafito ym. (2019) sivun 8 kuvio 2 sumulaskennan hierarkkiasta, jossa sumusolmut ovat sekä hajautettuna että yhdistettynä esineiden internetin laitetasolta ydinverkkoon saakka.
- **Kastelaskenta (Dew Computing, DC)** yhdistää pilvipalvelun pääkonseptin päätelaitteiden ominaisuuksiin. Sitä käytetään parantamaan loppukäyttäjän käyttökokemusta verrattuna pilvipalveluihin. Naha ym. (2018) mukaan kastelaskenta sijaitsee pilven ja sumutietokoneiden ympäristössä, perustuu mikropalveluihin, ja palvelee sensoreita, tabletteja ja matkapuhelimia, jotka ovat saumattomasti yhdistetty verkkoon ad-hoc-pohjaisilla ratkaisuilla. Esimerkiksi liikennevalojen välissä sijaitsevat älykkään liikenteenohjausjärjestelmän tiedonkeruu- ja käsittelylaitteet voivat luoda liikennetilanteen kokonaiskuvan, ja välittää sen autoille ajosuoritteen optimoimiseksi.
- **Usvalaskenta (Mist Computing)** kuvaa hajautettua tietojenkäsittelyä itse esineiden internetin laitteissa, ja sitä on ehdotettu ajatellen itsetietoisia ja autonomisia järjestel-

miä. Usvalaskenta voidaan nähdä ensimmäisenä laskentapaikkana esineiden internetin-sumupilven jatkumossa, ja sitä voidaan epävirallisesti kutsua termeillä ”esineiden internetin-tietojenkäsittely” tai ”laitteiden tietojenkäsittely”. Laite voi olla esimerkiksi puettava, mobiililaite, älykello, ajoneuvo tai älykäs jääkaappi. (Yousefpour ym. (2019).)



Kuvio 2. Sumulaskennan hierarkkinen rakenne (Puliafito ym. (2019) mukaillen).

Kuten listan lainauksista ja esimerkeistä voidaan päätellä, yksikäsitteisiä toisiaan poissulkevia käsitteitä ei löydy, vaan käsitteet ovat useasti päällekkäisiä ja jatkuvasti kehittyviä. Yhteistä listaan valituille käsitteille on mahdollisuus toimintaan itse tutkielman kohdelaitteessa, eli ajoneuvossa, tai sen avustamisessa, kuten liikenteenohjausjärjestelmässä. Näiden lisäksi ajoneuvot käyttävät yleisesti perinteisiä pilvipalveluja toimintaan, joka ei ole aikakriittistä tai vaatii suurta laskentatehoa, kuten miljoonien ajoneuvojen etähallintajärjestelmien toiminta. Reunalaskennan arkkitehtuurina käytetään yleisesti reuna- ja sumulaskennan kolmijakoa (Iorga ym. 2018; Puliafito ym. 2019; Yousefpour ym. 2019; Mahmood 2018; Xiao ym. 2019):

1. **Laitteet:** Esineiden internetin laitteet ovat yhdistettyjä laitteita, jotka tuottavat ja lähettävät erilaista strukturoitua ja osittain strukturoitua informaatiota.
2. **Sumu- tai reunaverkko:** Vastaanottaa reaaliaikaista tietoa esineiden internetin lait-

teista käyttämällä erilaisia viestintäprotokollien yhdistelmiä ja suorittaa reaaliaikaisen analyysin.

3. **Pilviympäristö:** vastaanottaa tietoja tallennettavaksi reunalaitteista / sumusolmuista ja myös suorittaa liiketoimintatiedon analysointia.

Reunalaskennan tietoturvan haasteellista toimintakenttää ja hyökkäyspintaa kuvaavat hyvin a) sumulaskennan hierarkkia, jossa sumusolmut ovat sekä hajautettuna että yhdistettynä esineiden internetin laitetasolta ydinverkkoon saakka, b) kolmijakoinen arkkitehtuuri laitteista pilvitasolle ja c) tiedonkäsittelyn jaettu strategia, jossa tietoa koostetaan ja käsitellään lähellä käyttäjää, eikä lähetetä kaikkea tietoa pilvikanavien kautta. Teknisesti pilvi- ja reunalaskenta eroavat toisistaan merkittävästi muun muassa osallistujien yhteyksien, laskentatehon, virrankäytön, erilaisten kyvykkyyksien, käsittelyn viiveen, liikkuvuuden tuen, tilatarpeen ja reaaliaikakäsittelyn mahdollisuuden suhteen. Keskeisimmät tekniset eroavuudet on koottu taulukkoon 1 sivulla 10.

Taulukko 1. Reunan ja pilven tekniset erot (Naha ym. (2018) mukaillen).

	Reunalaskenta	Pilvilaskenta
Osallistujat	Jatkuvasti vaihtuva	Vaihteleva
Hallinta	Hajautettu/Keskitetty	Keskitetty
Laskentalaite	Mikä tahansa prosessorivoimaa omaava	Voimakkaat palvelimet
Epäonnistumisen luonne	Erittäin vaihteleva	Ennustettava
Loppukäyttäjän yhteys	Enimmäkseen langaton	Suurnopeus (yhdistelmä langallista ja langatonta)
Sisäinen yhteystapa	Enimmäkseen langaton	Enimmäkseen langallinen
Virtalähde	Patteri/akku/suorasähkö/ aurinkovoima	Suorasähkö
Virrankulutus	Matala	Korkea
Laskentateho	Matala	Korkea
Tallennuskapasiteetti	Matala	Korkea
Virrankulutus	Matala	Korkea
Verkon viive	Matala	Korkea
Liikkuvuus	Korkea	Erittäin matala
Verkkohyppyjen määrä	Yksi/muutama	Usea
Sovellustyypit	Viivekriittiset	Ei-viivekriittiset
Reaaliaikakäsittely	Tehtävissä	Vaikea
Laskentahinta	Alhainen	Korkea
Jäähdytyskustannus	Erittäin alhainen	Korkea
Tilantarve	Vähäinen	Varastokeskuksen kokoinen rakennus

3 Reunalaskennan tietoturvahaasteita

Esineiden internetin laitteiden määrän ennustetaan kasvavan nopeammin kuin maapallon väestön tai internetin käyttäjien. Vuonna 2025 maailmassa ennustetaan olevan 40 miljardia älylaitetta, joiden välillä olisi 100 miljardia yhteyttä. Vuonna 2020 esineiden internetin, ihmisten ja esineiden tuottama dataliikenne oli kolmannes kaikesta, ja reunalla tuotetusta tiedosta 40 % analysoitiin, käsiteltiin ja tallennettiin verkon reunalla. (Cisco 2020; Huawei 2018; Zhang ym. 2018).

Reunalaskenta tarjoaa käyttökelpoisen laskentateknologian monille sovellusalueille, kuten älykkäät verkot, älykodit ja -kaupungit, itseohjautuvat autot, liikennevalojärjestelmät, terveydenhuolto, lääkinnälliset vaatteet ja teollisuuden ohjausjärjestelmät (Yousefpour ym. 2019; Naha ym. 2018; Mahmood 2018). Samalla reunalaskenta tuo Xiao ym. (2019) mukaan lisää turvallisuusuhkia, koska se lisää todellisen maailman hyökkäyspintaa seuraavista neljästä näkökulmasta.

- **Heikko laskentateho**: Pilvipalvelimeen verrattuna reunapalvelimen laskentateho on suhteellisesti heikompi. Reunapalvelin on siksi haavoittuvampi olemassa oleville hyökkäyksille, jotka eivät ehkä enää ole tehokkaita pilvipalvelinta vastaan. Samoin yleiskäyttöisiin tietokoneisiin verrattuna reunalaitteissa on hauraammat puolustusjärjestelmät, ja monet hyökkäykset, jotka voivat olla tehottomia pöytätietokoneita vastaan, voivat aiheuttaa vakavia uhkia reunalaitteisiin.
- **Hyökkäyksen huomaamattomuus**: Toisin kuin yleiskäyttöisissä tietokoneissa, useimmissa esineiden internetin laitteissa ei ole käyttöliittymiä, korkeintaan led-valoja. Käyttäjällä voi siksi olla vain vähän tietoa laitteen toimintatilasta, esimerkiksi onko se sammutettu tai vaarantunut. Useimmat käyttäjät eivät ehkä pysty havaitsemaan hyökkäyksiä reunalaitteisiin.
- **Käyttöjärjestelmien ja protokollien monimuotoisuus**: Toisin kuin yleiskäyttöisillä tietokoneilla, joissa on tapana käyttää vakiokäyttöjärjestelmiä ja -tietoliikenneprotokollia, useimmilla reunalaitteilla on erilaiset käyttöjärjestelmät ja protokollat ilman vakiintuneita tai standardoituja käytäntöjä. Tästä johtuen reunalaskennalle on vaikeaa suunnitella yhtenäistä suojamekanismia.

- **Karkearakeinen käyttöoikeuksien valvonta**: Yleiskäyttöisille tietokoneille ja pilvilaskentaan suunnitellut käyttöoikeuksien valvontamallit sisältävät pääasiassa neljän tyyppistä käyttöoikeutta: 1) Ei luku- tai kirjoitusoikeutta, 2) vain luku, 3) vain kirjoitus ja 4) luku- ja kirjoitusoikeus. Reunalaskennan monimutkaisemmat järjestelmät ja sovellukset vaativat hienorakeista oikeuksien valvontaa, jonka pitäisi käsitellä kysymyksiä, kuten "kuka pääsee käsiksi mihinkin sensoriin, tekemällä mitä, milloin ja miten". Nykyiset valvontamallit ovat enimmäkseen karkearakeisia (Fernandes, Jung ja Prakash 2016).

Esineiden internetin ja reunalaskennan hyökkäyspinta on kasvanut merkittävästi, samoin kuin mahdolliset uhkakuvat. Esimerkiksi teollisuuden turvallisuusuhat voivat johtaa tuhoisiin seurauksiin, ja autonomiset ajoneuvot ovat alttiita muun muassa sensoripohjaisille hyökkäyksille. Manipuloimalla esimerkiksi kiihtyvyys- tai magneettisia sensoreita hyökkääjät voivat kerätä tietoja, syöttää vääriä tai haitallisia tietoja, tai laukaista haitallisia toimintoja, kuten palvelunesto- tai sensorien energiankulutushyökkäyksen. (Krishna ym. (2021)).

3.1 Esimerkkejä toteutuneista tietoturvatapahtumista

Edellä mainituista syistä toteutuneita tietoturvatapahtumia luettelevat muun muassa (Euroopan unionin verkko- ja tietoturvavirasto 2017b; Xiao ym. 2019; Kuzlu, Fair ja Guler 2021) tutkimuksissaan ja tietoturvasuosituksissaan. Tapahtumista on poimittu muutama esimerkkitapahtuma ja -skenaario yleiskuvan saamiseksi:

- Mirai-virus onnistui saastuttamaan yli 65000 esineiden internetin laitetta ensimmäisten 20 tunnin aikana. Pian sen jälkeen Mirain ja sen lukuisten muunnosten uskottiin saaneen haltuunsa yli 378 miljoonaa laitetta. Laitteita käytettiin sulkemaan yli 178000 verkkotunnusta, ja ne vaikuttivat muun muassa Amazonin, Netflixin, Paypalin ja Spotifyn palveluihin. Havaittujen hyökkäysten vahinkojen arvon syyskuussa 2018 arveltiin olevan yli 100 miljoonaa dollaria.
- Tunnetun valmistajan auto otettiin haltuun kilometrien päästä, ja sille lähetettiin komentoja jotka vaikuttivat kojelaudan toimintoihin, ohjaukseen, jarruihin ja vaihteistoon. Kuljettaja ei voinut vaikuttaa ajoneuvon hallintaan ohjauksen tai polkimien kaut-

ta.

- Kahden asuinkorttelin lämmitysjärjestelmä kaadettiin palvelunestohyökkäyksellä, ja asukkaat jäivät pakkassäässä ilman lämmitystä yli viikoksi.
- Hotellin digitaalinen avainjärjestelmä otettiin haltuun – vieraat eivät enää päässeet hotellihuoneisiinsa eikä uusia avainkortteja voitu ohjelmoida. Hotelli myöntyi maksamaan tuhansien Bitcoinien arvoiset lunnaat tilanteen ratkaisemiseksi.
- Kalenteritiedot näyttävän älykkään jääkaapin haavoittuvuutta hyödyntäen varastettiin käyttäjän Google-tunnistetiedot.
- Kodin langattomat kamerat, itkuhälyttimet ja älylelut on pystytty ottamaan haltuun ja muuttamaan hyökkääjän käyttämiksi valvontalaitteiksi.
- Älykkäiden mittarien sähkönkulutuksesta on voitu päätellä kodissa tehtävät askareet, sekä vieraillut verkkosivut yli 99 % tarkkuudella.
- Tunnetun valmistajan älykkään kodin alustaa käyttäen on vaihdettu talon lukkojen koodit ja käynnistetty palohälyttimet.
- Älypuhelimen näppäilyt voidaan päätellä kiihtyvyysmittarin ja gyroskoopin anturei-den avulla, tai hyödyntäen etukameran kuvaa käyttäjän silmien liikkeestä.

Tietoturvan toteutuneet haasteet vaikuttavat jo laajasti miljoonien ihmisten elämään ja liiketoimintaan, ja voivat vaikuttaa yhteiskunnan toimivuuteen. Laitemäärän, palvelujen ja sovellusalueiden kasvaessa tietoturvan merkitys korostuu.

3.2 Uhkien luokitteluja ja yleisimpiä hyokkäystapoja

Tietoturvaan kohdistuvia uhkia luokitellaan usealla tavalla. Sengupta, Ruj ja Das Bit (2020) luokittelevat neljään pääluokkaan – 1) fyysiset-, 2) verkko-, 3) sovellus- ja 4) tietohyökkäykset, joista kaikilla on useampia alaluokkia. Roman, Lopez ja Mambo (2018) käyttävät jaottelua viiteen pääluokkaan laitetason mukaan – 1) verkkoinfrastruktuuri, 2) reunalaskentakeskus, 3) ydininfrastuuri, 4) virtualisointi-infrastuktuuri ja 5) loppukäyttäjien laitteet, joista jokaiselle on myös tarkemmat uhkakuvat.

Tässä tutkielmassa tukeudutaan luokittelussa Euroopan unionin verkko- ja tietoturvavirasto (2017b) tekemään uhkaluetteloon:

Taulukko: **Tietoturvauhkien luokittelu**
(Euroopan unionin verkko- ja tietoturvavirastoa mukaillen)

Kategoria	Uhka
Ikävä toiminta / väärinkäytökset	Haittaohjelmat
	Hyväksikäyttösarjat
	Kohdistetut hyökkäykset
	Palvelunestohyökkäykset
	Haitallisten laitteiden tekemät väärennökset
	Yksityisyyteen kohdistuvat hyökkäykset
	Tietojen muuttaminen
Salakuuntelu / Sieppaus / Kaappaus	Välimieshyökkäys
	Kommunikointiprotokollan kaappaus
	Tiedon sieppaus
	Verkon tutkiminen
	Istunnon kaappaus
	Tiedonkeruu
	Viestien toisto
Katkot	Verkkokatkot
	Laitevauriot
	Järjestelmäviat
	Tukipalvelujen menetys
Vahingot / IT-omaisuuden menetys	Arkaluontoisten tietojen vuoto
Virheet/häiriöt	Ohjelmistovirheet
	Kolmannen osapuolen virheet
Katastrofit	Luonnonkatastrofit
	Ympäristökatastrofit
Fyysiset hyökkäykset	Laitteen muuttaminen
	Laitteen tuhoutuminen (sabotaasi)

Tämän Euroopan unionin verkko- ja tietoturvaviraston luokittelun mukaisia uhkia määrittelevät muun muassa (Alwarafy ym. 2021; Euroopan unionin verkko- ja tietoturvavirasto 2017b; Alwakeel 2021; Kuzlu, Fair ja Guler 2021; Sengupta, Ruj ja Das Bit 2020; Xiao ym. 2019), yhdistettynä seuraavasti:

- **Haittaohjelma**: ohjelmisto, joka on suunniteltu suorittamaan ilman käyttäjän suostumusta ei toivottuja ja luvattomia toimintoja, jotka johtavat vaurioihin, vioittumiseen tai tietojen varastamiseen.
- **Hyväksikäyttösarja**: ohjelmakoodi, joka on suunniteltu hyödyntämään haavoittuvuutta päästäkseen järjestelmään.
- **Kohdistettu hyökkäys**: hyökkäys, joka on suunniteltu tiettyyn kohteeseen, toteutetaan useassa vaiheessa ja pitkän ajan kuluessa. Päätavoitteena on pysyä piilossa ja kerätä mahdollisimman paljon arkaluontoista tai hallintatietoa.
- **Palvelunestohyökkäys**: useampi järjestelmä hyökkää yhtä kohdetta vastaan tavoitteena ylikuormittaa ja kaataa se. Tämä voidaan tehdä tekemällä monia yhteyksiä, ylikuormittamalla viestintäkanavaa tai toistamalla samaa viestintää yhä uudelleen ja uudelleen.
- **Haitallisten laitteiden tekemä väärennös**: hyökkääjät joko ylikuormittavat tietoisesti verkon väärennetyillä viesteillä kuluttaakseen viestintä-, tietojenkäsittely- ja/tai tallennusresursseja, tai lähettävät harhaanjohtavia tietoja muuttaakseen järjestelmän toimintaa.
- **Yksityisyyteen kohdistuva hyökkäys**: uhka vaikuttaa joko käyttäjän yksityisyyteen, tai verkkoelementtien altistumiseen luvattomalle käytölle.
- **Tietojen muuttaminen**: tavoitteena ei ole vahingoittaa laitteita, vaan manipuloida tietoa aiheuttaakseen sekaannusta tai saadakseen rahallista hyötyä.
- **Välimieshyökkäys**: aktiivinen salakuunteluhyökkäys, jossa hyökkääjä välittää viestejä uhrilta toiselle, ja he uskovat puhuvansa suoraan toisilleen.
- **Kommunikointiprotokollan kaappaus**: olemassa olevan viestintäistunnon haltuunotto verkon kahden elementin välillä. Tunkeilija pystyy tarkastelemaan tietoja, mukaan lukien salasanat. Kaappauksessa voidaan käyttää aggressiivisia tekniikoita, kuten yhteyden katkaisua tai palvelun estoa.
- **Tiedon sieppaus**: luvaton tietojen sieppaus ja mahdollisesti muuttaminen yksityisvies-

tinnästä, kuten puheluista, pikaviesteistä tai sähköposteista.

- **Verkon tutkiminen**: hankitaan passiivisesti verkon sisäisiä tietoja, kuten verkkoon kytketyt laitteet, käytetyt protokollat, avoimet portit ja sisäisesti käytetyt palvelut.
- **Istunnon kaappaus**: tietoyhteyden varastaminen toimimalla laillisena isäntänä siirrettyjen tietojen varastamiseksi, muokkaamiseksi tai poistamiseksi.
- **Tiedonkeruu**: hankitaan passiivisesti verkon sisäisiä tietoja kuten kytketyt laitteet, käytetyt protokollat, avoimet portit ja sisäisesti käytetyt palvelut.
- **Viestien toisto**: hyökkäys käyttää kelvollista tiedonsiirtoa haitallisesti, lähettäen sen toistuvasti tai lykäten sen lähettämistä, tarkoituksena manipuloida tai kaataa kohdelaite.
- **Verkkokatko**: verkkopalvelujan tahallinen tai vahingossa tapahtunut katkos tai vika.
- **Laitevaurio**: laitteiston vian tai toimintahäiriön uhka.
- **Järjestelmävika**: ohjelmistopalvelujen tai sovellusten epäonnistumisen uhka.
- **Tukipalvelujen menetys**: tietojärjestelmän asianmukaisen toiminnan takaamiseksi tarvittavien tukipalvelujen puuttuminen.
- **Arkaluontoisten tietojen vuoto**: arkaluonteisia tietoja paljastetaan luvattomille osapuolille vahingossa tai tahallaan.
- **Ohjelmistovirheet**: heikot- tai oletussalasanat, ohjelmistovirheet ja määrittelyvirheet, jotka aiheuttavat haavoittuvuusriskin, joita voidaan hyödyntää muihin tarkoituksiin.
- **Kolmannen osapuolen virhe**: verkon aktiivisessa elementissä tapahtuva virhe, joka johtuu siihen suorassa suhteessa oleva toisen elementin virheellisestä määrittelystä.
- **Luonnonkatastrofi**: tapahtumat, kuten tulvat, kovat tuulet, ja maanvyörymät, jotka voivat vaurioittaa laitteita fyysisesti.
- **Ympäristökatastrofi**: tapahtumat esineiden internetin käyttöympäristössä, jotka voivat vahingoittaa laitteita ja aiheuttaa niiden toimintakyvyttömyyden.
- **Laitteen muuttaminen**: laitteen peukalointi esimerkiksi hyödyntämällä auki jätettyjä verkkoportteja.
- **Laitteen tuhoutuminen**: laitteista vahingoittavat tapahtumat, kuten varkaudet, pommiiskut, ilkivalta tai sabotaasi.

Tämän tutkielman työmäärän puitteissa kaikkia Euroopan unionin verkko- ja tietoturvaviraston luokittelun mukaisia uhkia ja niihin johtavia hyökkäystyyppejä ei ole mahdollista käydä

lävitse. Kirjallisuudesta löytyy myös muita uhkamainintoja, ja kokemusperäisesti on helppo sanoa, että Euroopan unionin verkko- ja tietoturvaviraston luokittelu ei myöskään ole kaikenkattava. Esimerkiksi artikkelissaan “Security Controls for Smart Buildings with Shared Space” Frantti ja Korkiakoski (2022) täydentävät luetteloa useassa kohdassa.

Kirjallisuudesta ja tilastoinnista löytyy taustatietoa, joka auttaa kohdistamaan tutkimusta reaalimaailmassa tapahtuviin uhkiin ja hyökkäystapoihin.

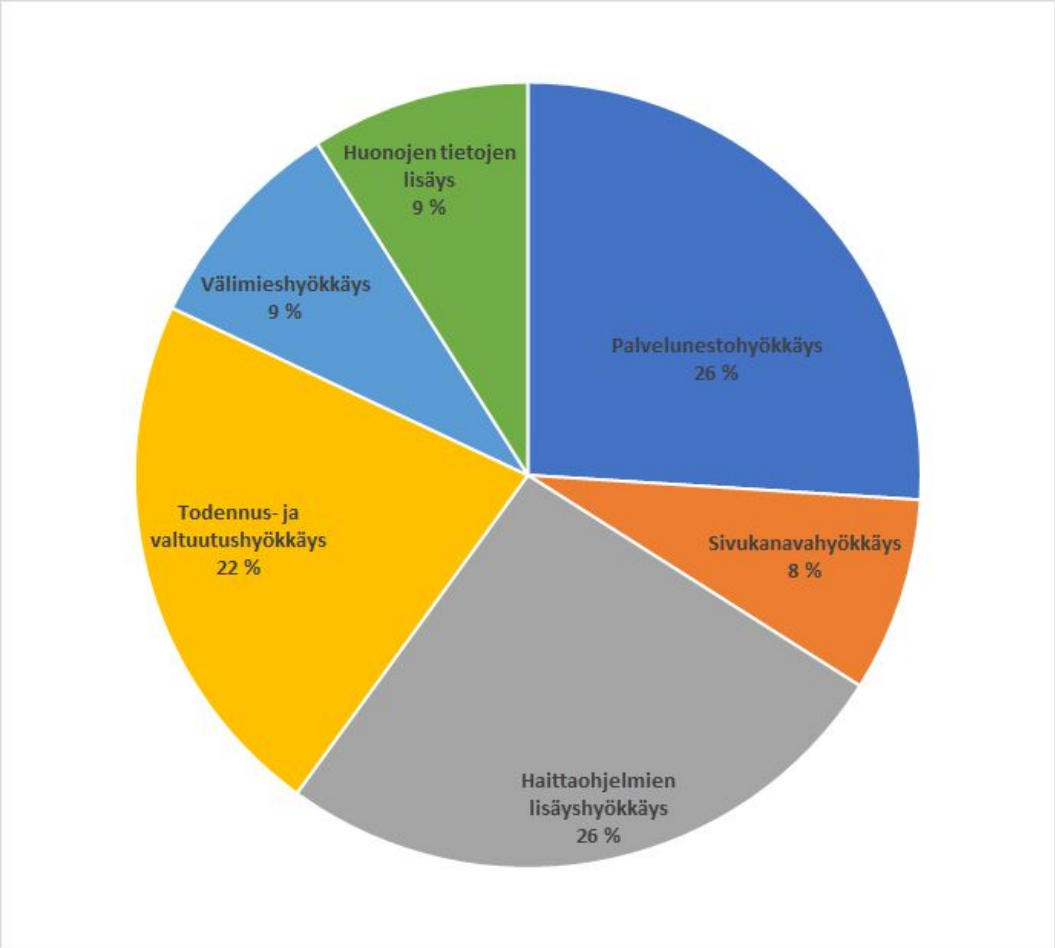
Xiao ym. (2019) mukaan tärkeimmät reunalaskentaan sovellettavat hyökkäykset luokitellaan kuuteen luokkaan:

1. palvelunestohyökkäys (Distributed Denial of Service, DDoS),
2. sivukanavahyökkäys (side-channel attack),
3. haittaohjelmien lisäyshyökkäys (malware injection),
4. todennus- ja valtuutushyökkäys (authentication and authorization),
5. välimieshyökkäys (man-in-the-middle, MITM) ja
6. huonojen tietojen lisäys (bad-data injection)

Vuonna 2017 löydettyjen esineiden internetin hyökkäysten kokonaismäärä on 159 700, joista lähes kaikki kuuluvat näihin kuuteen luokkaan. Näiden hyökkäysluokkien prosenttiosuudet Statistan raportin mukaan on esitetty kuviossa 3. (Xiao ym. (2019).) On huomautettava, että tilastoinnista johtuen erilaisia tapauslukuja esiintyy, esimerkiksi McAfee Labs havaitsi Ni, Lin ja Shen (2019) mukaan yli 1,5 miljoonaa mobiilihaittaohjelmien aiheuttamaa tapausta vuoden 2017 kolmen ensimmäisen kuukauden aikana. Otoum, Liu ja Nayak (2019) mainitsevat SonicWallin vuoden 2019 kyberuhat-raportin mukaan hyökkäysten lisääntyneen vuoden 2018 aikana 217,5 %, vuoden 2017 10,3 miljoonasta 32,7 miljoonaan.

3.3 Yleisimpien hyökkäystyyppien kuvaus

Luvussa kuvataan yleisimmät kuusi hyökkäystyyppiä yleistasolla, ilman tekniikka- tai protokollatason tarkkoja yksityiskohtaisia teknisiä läpikäyntejä. Yksityiskohtainen tarkastelu on eri tekniikoiden moninaisuuden takia rajattu tämän tutkielman ulkopuolelle.



Kuvio 3. Reunalaskennan toteutuneet hyökkäystyypit 2017 (Xiao ym. (2019) mukaillen).

3.3.1 Palvelunestohyökkäys

Palvelunestossa hyökkääjä pyrkii katkaisemaan yhden tai useamman palvelimen normaalit palvelut käyttäen hajautettuja resursseja, kuten haltuunotettujen reunalaitteiden klusteria (tunnetaan myös nimellä botnet). Hyökkääjä murtautuu ensin reunalaitteiden klusteriin ja ottaa laitteet täysin hallintaansa, jonka jälkeen käsketään jokaista laitetta käynnistämään palvelunestohyökkäys reunapalvelimeen, mikä aiheuttaa sen palveluiden sulkemisen. (Xiao ym. (2019) ja Kuzlu, Fair ja Guler (2021).) Palvelunestohyökkäykset käyvät Kuzlu, Fair ja Guler (2021) mukaan yleensä läpi muutaman vaiheen: 1) rekrytointi, jossa hyökkääjä etsii haavoittuvia koneita käytettäväksi, 2) hyväksikäyttö ja infektio, jossa haavoittuvia koneita käytetään hyväksi ja haittakoodi syötetään, 3) viestintä, jossa hyökkääjä arvioi tartunnan saaneet koneet, näkee mitkä ovat saatavilla ja päättää milloin hyökkäykset ajoitetaan tai koneet päivitetään, ja 4) hyökkäys, jossa hyökkääjä käskee tartunnan saaneita koneita lähettämään haitallisia paketteja kohteeseen.

Perinteinen palvelunestohyökkäys tapahtuu, kun hyökkääjä lähettää jatkuvasti pakettivirtoja uhrille hajautetuista laitteista. Tällöin uhrin laitteistoresurssit kuluvat nopeasti loppuun haitallisten pakettien käsittelyssä, eikä laillisia pyyntöjä pystytä käsittelemään ajoissa. Toisessa skenaariossa hyökkääjä lähettää jatkuvasti väärin muotoiltuja paketteja, jotka sekoittavat uhrin sovelluksen tai protokollan päättelemään virheellisesti, että kaikki kanavat ja resurssit ovat varattuja. Pilvipalvelimiin verrattuna reunapalvelimet ovat alttiimpia palvelunestohyökkäyksille, koska ne ovat suhteessa laskennallisesti vähemmän tehokkaita ylläpitämään vahvoja (pilvipalvelinten) puolustusjärjestelmiä. Lisäksi reunapalvelimet tarjoavat palveluita pääasiassa reunalaitteisiin, joiden tiedetään olevan tietoturva-asetuksissa virhealttiita laskentarajoitteisen laitteistonsa ja monimuotoisen laiteohjelmistonsa vuoksi. (Xiao ym. (2019), Alwakeel (2021) ja Kuzlu, Fair ja Guler (2021).)

Reunalaskentaan kohdistuvat palvelunestohyökkäykset voidaan luokitella kuormitushyökkäyksiksi (flooding) ja nollapäivähyökkäyksiksi (zero-day). Kuormitushyökkäys perustuu suureen määrään virheellisesti muotoiltuja tai haitallisia verkkopaketteja, ja ne luokitellaan pääasiassa protokollan mukaisesti UDP-, ICMP-, SYN-, HTTP-kuormituksiksi, TearDrop, Land Attack, kuoleman pingiksi (Ping-of-Death, PoD) tai työkalun mukaan esimerkiksi Slowloris-kuormitukseksi. (Xiao ym. (2019) ja Lin ym. (2017).) Hyökkääjä voi Sengupta,

Ruj ja Das Bit (2020) mukaan kaapata kelvollisen allekirjoitetun paketin ja lähettää paketin uudelleen useita kertoja määränpäähän ja siten kuormittaa verkon. Nollapäivähyökkäys on edistyneempi kuin kuormitushyökkäys, mutta vaikeampi toteuttaa. Nollapäivähyökkäyksessä hyökkääjän on löydettävä tuntematon haavoittuvuus (eli nollapäivän haavoittuvuus) reunapalvelimella tai -laitteella ajettavasta koodinpätkästä, joka voi aiheuttaa muistin vioittumisen ja lopulta palvelun sulkemisen. (Xiao ym. (2019).)

Reunalaitteet voivat usein suorittaa palvelunestohyökkäyksiä, mutta ne ovat myös itse alttiita niille. Reunatoimijat ovat erityisen alttiita pysyville palvelunestohyökkäyksille (Permanent DoS), jotka tekevät laitteen tai järjestelmän täysin toimintakyvyttömäksi. Tämä voidaan tehdä ylikuormittamalla akkua, virtajärjestelmää tai yleisemmin laiteohjelmistohyökkäyksillä. Laiteohjelmistohyökkäyksessä hyökkääjä voi käyttää haavoittuvuuksia korvatakseen (phlashing) laitteen perusohjelmiston (yleensä sen käyttöjärjestelmän) vioittuneella tai viallisella ohjelmistoversiolla, mikä tekee siitä hyödyttömän. Tällöin laitteen omistajalla ei ole muuta vaihtoehtoa kuin alustaa laite puhtaalla kopiolla käyttöjärjestelmästä ja sisällöstä, joka on saatettu laittaa laitteeseen. Erityisen voimakkaassa hyökkäyksessä vioittunut ohjelmisto voi ylikuormittaa laitteen laitteistoa siten, että palautus on mahdotonta ilman laitteen osien vaihtamista. Yksi tunnetuimmista haittaohjelmista on BrickerBot, joka käyttää raa'an voiman sanakirjahyökkäyksiä päästäkseen käsiksi laitteisiin, ja suorittaa laitteeseen kirjautumisen jälkeen sarjan komentoja, jotka johtavat laitteen pysyvään vaurioitumiseen. Näitä komentoja ovat muun muassa laitteen tallennustilan ja ytimen parametrien virheellinen määritys, Internet-yhteyden estäminen, laitteen suorituskyvyn sabotointi ja kaikkien laitteessa olevien tiedostojen pyyhkiminen. (Kuzlu, Fair ja Guler (2021) ja Sengupta, Ruj ja Das Bit (2020).) Katkoshyökkäykset, unenriisto ja akun tyhjennys ovat Alwarafy ym. (2021) mukaan tunnetuimpia palvelunhyökkäystyyppejä reunan toimijoita vastaan. Katkoshyökkäyksissä ne lakkaavat suorittamasta normaalia toimintaansa, koska ne ovat altistuneet luvattomalle käytölle. Unen puutteessa laitteet kuormitetaan ei-toivotuilla laillisilla pyynnöillä, ja hyökkäys on paljon vaikeampi havaita. Akun tyhjentyessä reunasolmujen tai sensorien/laitteiden akku tyhjenee, ja tapahtuu vika tai katkos. Viestinnän tasolla yleisin hyökkäys on kuitenkin signaalien lähetyksen häirintä, joka sisältää 1) jatkuvan häirinnän kaikissa lähetyksissä ja 2) ajoittaisen häirinnän lähettämällä/vastaanottamalla paketteja ajoittain. (Alwarafy ym. (2021)). Radiotaajuushäirintä on Sengupta, Ruj ja Das Bit (2020) mukaan yleistä. Siinä hyökkääjä luo

ja lähettää kohinasignaaleja radiotaajuisten (Radio Frequency, RF) signaalien kautta estäen reunalaitteiden viestinnän.

3.3.2 Sivukanavahyökkäys

Sivukanavahyökkäyksessä vaarannetaan käyttäjän turvallisuus ja yksityisyys käyttämällä mitä tahansa julkisesti saatavilla olevaa tietoa, joka ei ole luonteeltaan arkaluonteista, eli sivukanavan tietoja. Tällainen julkinen tieto korreloidaan tyypillisesti ”salaisesti” tiettyjen yksityisyyden kannalta suojattavien arkaluontoisten tietojen kanssa. Hyökkääjät tutkivat sitten piilotettuja korrelaatioita päätelläkseen lopulta suojatut tiedot sivukanavista. Koska kaikki julkiset tiedot voivat linkittyä joihinkin arkaluontoisiin tietoihin, sivukanavahyökkäyksiä voi tapahtua missä tahansa reunalaskenta-arkkitehtuurissa. (Xiao ym. (2019).) Tutkimuksissaan (Alwakeel 2021; Parikh ym. 2019) määrittelevät reunalaskennassa sivukanavahyökkäykseksi laitteen kryptografian avaamisen keräämällä tietoja käytetystä salausalgoritmista.

Xiao ym. (2019) mukaan hyökkääjä hankkii jatkuvasti tiettyjä sivukanavatietoja kohdereunan laskentainfrastruktuurista ja syöttää ne sitten koneoppimismalleihin tai algoritmeihin, jotka tuottavat halutut arkaluontoiset tiedot. Reunalaskennan suosituimpia sivukanavia ovat viestintäsignaalit, sähkönkulutus, älypuhelimen tiedostojärjestelmä (/proc) ja sulautetut sensorit. Viestintäkanavia hyödyntävät hyökkäykset tapahtuvat, kun hyökkääjä tarkkailee jatkuvasti kahden reunasolmun välistä lähetystä. Virrankulutusta hyödyntävät hyökkäykset tapahtuvat hyökkääjän varastettua reunalaitteiden virrankulutustiedot. Älypuhelinpohjaisia kanavia hyödyntävät hyökkäykset tapahtuvat, kun hyökkääjä käyttää salaa älypuhelinta, ja varastaa julkisesti saatavilla olevaan /proc-tiedostoon tallennetun tai sulautettujen antureiden luoman tiedon. Sivukanavat voidaan luokitella kahteen luokkaan: hallittaviin, kuten sensoritiedot, joihin pääsyä voidaan rajoittaa, ja hallitsemattomiin, kuten aaltosignaalit, joita luonteensa vuoksi ei voida muuttaa.

Reunalaskennassa viestintäsignaalien hyödyntämisellä on suuri mahdollisuus paljastaa uhrin arkaluontoisia tietoja runsaan kanavainformaation ansiosta. Tässä tapauksessa hyökkääjä voi olla mikä tahansa utelias haitallinen solmu (jonka ei tarvitse olla reunalaite tai reunapalvelin), joka haistelee jatkuvasti verkkojälkiä ja poimii niistä arkaluonteisia tietoja. (Xiao

ym. (2019)). Esimerkiksi tunnettujen sähkömagneettisten/akustisten signaalien tai protokollien havaitseminen lääkinnällisistä laitteista voi johtaa kriittisen tiedon vuotamiseen potilaasta ja laitteesta (Alwarafy ym. 2021; Mosenia ja Jha 2017). Viestintäsignaalia hyödyntävät sivukanavahyökkäykset voidaan jakaa kahteen alaluokkaan: pakettivirtoja hyödyntäviin ja aaltosignaaleja hyödyntäviin.

Paketti on perusyksikkö useimmissa viestintäkanavissa. Joukko paketteja sisältää runsaasti tietoa, ja siksi hyökkääjät käyttävät niitä laajasti hyväkseen päätelläkseen arkaluontoisia tietoja. H. Li ym. (2016) osoittivat että esimerkiksi H.264:n ja MPEG-4:n käyttämä koodausmenetelmä voi aiheuttaa vakavan yksityisyyden vuodon kodin valvonnassa, vaikka videovirta olisikin salattu. Käyttämällä yksinkertaisia koneoppimisalgoritmeja, voidaan saavuttaa jopa 95,8 %:n tarkkuus ihmisen päivittäisen toiminnan, kuten pukeutumisen, hiusten muotoilun, liikkumisen ja syömisen, päättelemisessä. Useimmat langattomat reitittimet vastaavat erilaisiin TCP-paketteihin erilaisilla ajoituseroilla, jonka vuoksi hyökkääjä voi päätellä oikean TCP-pakettinumeron ja suorittaa TCP-pakettien lisäyshyökkäyksiä. (Xiao ym. (2019).)

Aaltosignaalit ovat toisen tyyppisiä sivukanavia viestintäprosessissa. Yksi merkittävistä esimerkeistä on sähkömagneettinen häiriö (electromagnetic interference, EMI). Selvaraj ym. (2018) ovat osoittaneet, että tarkoituksellisen sähkömagneettisen häiriön avulla hyökkääjä voi manipuloida sensorilaitteen tulo- ja lähtösignaaleja fyysisestä kerroksesta ja ohittaa perinteiset eheyden tarkistusmekanismit. Langattoman verkon liikennettä voidaan käyttää sivukanavina johtopäätöshyökkäysten tekemiseen, esimerkiksi hyödyntämällä kanavan tilatietojen (Channel State Information, CSI) muutoksia uhrin arkaluontoisen salasanan, kuten Alipay-koodin, päättelemiseksi sormen liikkeiden perusteella. (Mosenia ja Jha (2017), M. Li ym. (2016), Xiao ym. (2019).)

Tehonkulutus on osoitus järjestelmän sähkönkäytöstä. Se sisältää tietoja, joko energiaa kuluttavasta laitteesta, koska eri laitteilla on erilaiset virrankulutusprofiilit toimiessaan, tai laskutoimitusten intensiteetistä laskentatehtävässä. Tehonkulutukseen perustuvat hyökkäykset jaetaan kahteen alaluokkaan: hyökkäyksiin, joissa hyödynnetään mittarien keräämää virrankulutusta, ja hyökkäyksiin, jotka käyttävät hyväkseen oskilloskooppien keräämää virrankulutusta. (Xiao ym. (2019).)

Älykkäät mittarit voivat Xiao ym. (2019) mukaan mitata tarkasti kotitalouden sähkönkulutuksen. Useimmat kotitaloustoiminnot, kuten ruoanlaitto, pyykinpesu, television katseleminen ja pelaaminen, voidaan päätellä älykkäiden mittarien infrastruktuurin energiatiedoista. Hyödyntämällä reunalaitteen virrankulutusta voidaan päätellä laitteen vierailema verkkosivu noin 99 prosentin tarkkuudella. Tällä tekniikalla voidaan toisaalta havaita haittaohjelmat reunalaitteessa noin 94 % tarkkuudella. (Clark ym. 2013).

Oskilloskooppi mittaa laitteiston elektronisia tietoja, esimerkiksi jännitettä ja virtaa. Nykyaikaisissa sulautetuissa laitteissa jotkut sirut voivat suorittaa monimutkaisia salausalgoritmeja, ja sirussa on kovakoodattu salainen avain. Tällaista salaista avainta ei voida murtaa suoraan, jos siinä ei ole ohjelmistotason haavoittuvuuksia. Örs, Oswald ja Preneel (2003) mukaan yksinkertaisen tehoanalyysin ja differentiaalisen tehoanalyysin avulla voidaan paljastaa huomattava määrä informaatiota, jota sirun salausjärjestelmä käsittelee. Korrelaatiotehoanalyysilla voidaan päätellä esimerkiksi pääsalausavain, jota käytetään Philipsin älyvalojärjestelmän salaukseen ja purkuun, ja hyödyntää sitä haittaohjelmiston asentamiseen (Ronen ym. 2017). Tutkijat raportoivat, että lähes kaikki kryptografiset lähestymistavat ja niitä vastaavat laitteistot ovat alttiina tehoanalyysihyökkäyksille. Tehoanalyysihyökkäysten käynnistäminen vaatii kuitenkin hyökkääjältä pääsyn kohdelaitteeseen haitallisen sovelluksen kautta tai fyysisesti, mikä vaikeuttaa tällaisten hyökkäysten toteuttamista. (Xiao ym. (2019).)

Älypuhelimet ovat tärkeitä laitteita monissa reunan sovelluksissa. Älypuhelimissa on Xiao ym. (2019) mukaan perinteisiä esineiden internetin laitteita edistyneemmät käyttöjärjestelmät ja rikkaammat järjestelmätiedot, ja ne voivat altistua laajemmalle hyökkäyspinnalle. Hyökkäykset luokitellaan kahteen alaluokkaan: /proc-tiedostojärjestelmää käyttävät, ja älypuhelimen upotettuja sensoreita käyttäviin.

/proc on Linuxin ytimen luoma järjestelmätason tiedostojärjestelmä, joka sisältää järjestelmätiedot, kuten keskeytys- ja verkkotiedot. Vaikka se on järjestelmätason tiedostojärjestelmä, käyttäjätason säikeet ja sovellukset voivat lukea sen, eikä sen käyttäminen vaadi lisäoikeuksia. Sivukanavahyökkäyksillä voidaan suorittaa muun muassa käyttöliittymän tietojenkalastelua ja huijata uhreja tekemään ei-toivottuja pyyntöjä reunapalvelimille, ja päätellä käyttäjän arkaluontoisia tietoja, kuten terveydentila, sijainti ja sosiaalisen verkoston identiteetti. /proc-käyttö edellyttää haitallisen sovelluksen asentamista. (Chen, Qian ja Mao

(2014), Zhou ym. (2013) ja Xiao ym. (2019).)

Nykyään älypuhelimeen on integroitu useita upotettuja sensoreita avustamaan käyttäjiä ja parantamaan toimintoja. Niihin liittyy kuitenkin arkaluontoisten tietojen vuotoriskejä. Tutkijat ovat esimerkiksi murtaneet älypuhelimen kuviolukon hyödyntämällä mikrofonien läpi siepatun sormenpään heijastamia akustisia signaaleja, ja osoittaneet, että näppäilyt voidaan päätellä älypuhelimen kiihtyvyysmittarin ja gyroskoopin antureiden avulla. (Xiao ym. (2019).)

3.3.3 Haittaohjelmien lisäyshyökkäys

Haittaohjelmien lisäyshyökkäykseksi kutsutaan toimintaa, jossa salassa syötetään tai asennetaan tietokonejärjestelmään haitallisia ohjelmistoja. Perinteisissä pilvi- tai yleiskäyttöisissä tietokoneratkaisuissa on saatavilla laskentatehoa esimerkiksi korkean suorituskyvyn palomuurin tukemiseksi, eikä haittaohjelmien lisääminen ei ole aina hyökkääjän kannalta järkevää tai mahdollista. Kaikkia reunalaitteita ja reunapalvelimia tuskin voidaan suojata perinteisellä palomuurilla, ja ne ovat alttiimpia haittaohjelmien lisäyshyökkäyksille. Reunalaskennan lisäyshyökkäykset jaetaan kahteen luokkaan: 1) reunapalvelimiin kohdistuviin ja 2) reunalaitteisiin kohdistuviin hyökkäyksiin.

Xiao ym. (2019) mukaan reunapalvelimiin kohdistuvia lisäyshyökkäyksiä on pääasiassa neljää tyyppiä: 1) kyselykielen lisäys (SQL-injection), 2) verkkosivustojen väliset komennot (Cross-Site Scripting, XSS), 3) verkkosivustojen välisten pyyntöjen väärennös (Cross-Site Request Forgery, CSRF) ja palvelinpyynnön väärennös (Server-Side Request Forgery, SSRF), ja 4) merkintäkielen allekirjoituskääreet (Extensible Markup Language (XML) signature wrapping).

Kyselykielen lisäys on koodin lisäystekniikka, joka tuhoaa taustatietokannat. Normaalin tietokantakyselyn muodostamiseksi laillinen käyttäjä saa käsitellä vain määritettyjä alueita (kuten nimeä ja päivämäärää) saadakseen tulokset palvelimelta. Hyökkääjä saattaa kuitenkin onnistua kiertämään tämän rajoituksen syöttämällä koodinvaihtomerkkejä (escape characters), kuten lainausmerkkejä, kyselymerkkijonon mukana. Tällöin palvelin saattaa vahingossa suorittaa kaiken, mitä hyökkääjä syöttää koodinvaihtomerkkien jälkeen, ja siten esimerkiksi muuttaa käytettävää tietokantaa tai jopa palvelimen toimintaa. (Xiao ym. (2019) ja

Krishna ym. (2021).)

Verkkosivustojen välinen komentohyökkäys on reunapalvelimen asiakaspuolen hyökkäys, jossa hyökkääjä lisää haitallisia koodeja (yleensä HTML/JavaScript-koodeja) tietosisältöön, jota palvelimet voivat käyttää ja suorittaa automaattisesti. Muutoin luotettava reunapalvelin toimii ”asiakkaana” vieraillakseen tai käyttääkseen muiden reunapalvelimien tai pilven tarjoamia palveluita. Hyökkäyksessä reunapalvelimet eivät suodata koodia datasisällöstä, johtaen hyökkääjän koodien suorittamiseen. (Xiao ym. (2019) ja Krishna ym. (2021).)

Verkkosivustojen välisten pyyntöjen väärennöksessä reunapalvelin pakotetaan suorittamaan ei-toivottuja toimintoja verkkosovellusten kautta, ja lukemaan tai muuttamaan sisäisiä resursseja. Varmennusmekanismin karkeudesta, kuten heikosta henkilöllisyyden todennusmenetelmästä, johtuen hyökkääjä voi huijata ”laillisena” reunapalvelimena ja lähettää komentoja muille reunapalvelimille ilman että ne havaitsevat laitonta toimintaa. (Xiao ym. (2019).)

Merkintäkielen allekirjoituksessa hyökkääjä sieppaa ensin laillisen viestin, luo uuden tunnisteen ja asettaa kopion alkuperäisestä viestistä (joka voi sisältää vahvistusparametreja, kuten tunnuksia) uuteen kääreeseen (wrapper). Muuttamalla alkuperäisen viestin arvoja kopiossa haitallisilla koodeilla, ja sijoittamalla jo vahvistetun viestin kääreeseen mukaan, hyökkääjä saa palvelimen suorittamaan haitallisen koodin. (McIntosh ja Austel (2005) ja Xiao ym. (2019).)

Reunalaitteiden ollessa erittäin monimuotoisia sekä laitteiden että laiteohjelmistojen osalta, on olemassa useita erilaisia menetelmiä haittaohjelmien lisäämiseksi laitteisiin. Yleisin tapa lisätä haittaohjelmia etänä on hyödyntää nollapäivän haavoittuvuuksia, jotka voivat johtaa koodin etäsuorittamiseen (Remote Command Execution, RCE) tai komentojen lisäämiseen. (Xiao ym. (2019).) 2017 Reaper-virus saastutti miljoonia reunalaitteita hyödyntämällä vähintään 30 etäsuoritushaavoittuvuutta yhdeksässä eri reunalaitteessa, kuten verkkoreitittimet ja IP-kamerat (Greenberg 2017).

Ristiinpääsyn mahdollistavien haittaohjelmien lisääminen mobiililaitteisiin ei ole yksinkertaista, sillä suuret mobiilikäyttöjärjestelmät, kuten iOS ja Android, käyttävät sovellusten eristys- eli hiekkalaatikkomekanismia varmistaakseen, että jokainen sovellus on omassa muistialueessaan eikä sovellus voi käyttää muiden sovellusten resursseja ja sisältöä, ellei ydintaso

(kernel) sitä salli. Sovelluskaupoista löytyy edelleen sovelluksia ja niiden käyttämiä kirjastoja, jotka avaavat takaoven koodin lisäämiselle. Aina ei tarvita edes asennusta, vaan jopa vierailu verkkosivulla voi hyödyntää käyttöjärjestelmän komponenttien haavoittuvuuksia ohjelmakoodin suorittamiseen. (Google (2022a), Apple (2021) ja Xiao ym. (2019).)

3.3.4 Todennus- ja valtuutushyökkäys

Todennus on toiminto, jolla varmistetaan palveluita pyytävien käyttäjien identiteetit. Valtuutus on prosessi, jossa määritetään käyttäjän pääsy- ja käyttöoikeudet, sekä varmistetaan, ettei käyttäjä ylitä oikeuksiensa rajoja. Reunalaskennassa todennus suoritetaan yleensä reunalaitteiden ja reunapalvelimien välillä. Tietyissä olosuhteissa todennus suoritetaan myös reunalaitteiden tai reunapalvelimien välillä hajautetusti, yleensä käyttämällä automaatioalustoja eli laukaisu-toiminta-alustoja (trigger-action). (Xiao ym. (2019) ja Istiaque Ahmed ym. (2021).) Laukaisu-toiminta-alustat ovat verkkopohjaisia järjestelmiä, joiden avulla voidaan luoda automaatiosääntöjä yhdistämällä digitaalisia ja fyysisiä resursseja edustavia verkkopalveluita OAuth-käyttäjätunnuksien avulla (Fernandes ym. 2018)). Reunalaskennan valtuutus viittaa usein toimintaan, kun reunapalvelin myöntää oikeudet tietylle reunalaitteelle tai sen sovelluksille. Laukaisutoimintoskenaariossa laitteet ja sovellukset voivat myös myöntää käyttöoikeuksia muille laitteille ja sovelluksille, esimerkiksi kodin automaatiojärjestelmälle. (Xiao ym. 2019; Istiaque Ahmed ym. 2021).

Yleensä reunalaskennan laitepohjainen todennus ja valtuutus käyttävät toimijalle tallennettuja asiakaspuolen varmenteita, ja varmennus tapahtuu TLS (Transport Layer Security) -kättelyssä. Osana kättelyä toimija lähettää valmiiksi määritetyn allekirjoitusviranomaisen allekirjoittaman varmenteensa käyttäen yksityistä avaintaan. Kättelyn lopussa toimija varmistetaan ja asiakastunnus poistetaan varmenteesta. Kun toimija on varmennettu, asiakastunnus on tiedossa ja sen avulla voidaan määrittää oikeat valtuutus- ja käyttöoikeusryhmät. (Istiaque Ahmed ym. (2021).)

Viereiset reunasolmut kommunikoivat yleensä keskenään jakaakseen tietojaan. Jos hyökkääjä pääsee johonkin suojaamattomista reunasolmuista, on mahdollista hallita kaikkia naapurisolmuja. (Alwarafy ym. (2021).) Solmun sieppaushyökkäyksessä hyökkääjä vaihtaa fyysi-

sesti koko solmun tai käsittelee ohjelmistoa tai laitteistoa. Tällöin tärkeä tieto, kuten ryhmäviestintäavain, voi paljastua hyökkääjälle. Replikointihyökkäyksessä hyökkääjä kopioi siepattuihin solmuihin liittyvät tärkeät tiedot haitalliseen solmuun tehdäkseen tästä valtuutetun, joka kykenee jopa peruuttamaan laillisten reunasolmujen valtuuksia. (Lin ym. (2017) ja Alwarafy ym. (2021).)

Hyökkäykset luokitellaan Xiao ym. (2019) mukaan neljään tyyppiin: 1) sanakirjahyökkäykset, 2) todennusprotokollien haavoittuvuuksia hyödyntävät hyökkäykset, 3) valtuutusprotokollien haavoittuvuuksia hyödyntävät hyökkäykset ja 4) ylioikeutetut hyökkäykset. Näistä kaksi ensimmäistä kohdistuvat todennusprotokolliin ja loput valtuutusprotokolliin.

Sanakirjahyökkäyksessä hyökkääjä käyttää valtuustieto-/salasanasanakirjaa murtaakseen tunnistetietoja käyttävän todennusjärjestelmän. Hyökkääjä käyttää sanakirjaa, joka sisältää useimmiten käytetyt tunnistetiedot/salasanat, ja syöttää kaikki mahdolliset tässä sanakirjassa olevat tiedot kohdetodennusjärjestelmään löytääkseen mahdollisen vastaavuuden. Tämäntyyppiset hyökkäykset tunnetaan myös väsytyshyökkäyksinä (brute-force). (Xiao ym. (2019).) Tutkimuksessaan Roy ym. (2018) ovat osoittaneet, että myös biometriset tunnisteet ovat alttiita sanakirjatyyppiselle hyökkäykselle.

Hyökkäyksissä, joissa hyödynnetään todennus- ja valtuutusprotokollien heikkouksia, käytetään reunalaskennassa yleensä WPA/WPA2-, SSL/TLS- ja OAuth-protokollia. Myös 4G ja 5G protokollista on löydetty vastaavia heikkouksia, joilla esimerkiksi lailliselta käyttäjältä voidaan evätä 4G-palvelut, käynnistää välimieshyökkäys paljastaen arkaluontoista tietoa tai nähdä uhrin sijainnin. Reunalaskentajärjestelmissä OAuth on laajalti käytetty valtuutusprotokolla, joka on suunniteltu monen osapuolen valtuutukseen. Siinä mukana on kolme osapuolta, eli käyttäjä, palveluntarjoaja ja luottavainen osapuoli. OAuthin tarkoituksena on antaa palveluntarjoajalle (esimerkiksi sovellukselle tai verkkosivulle) pääsy luottavan osapuolen hallitsemiin käyttäjän tietoihin vasta käyttäjän myönnettyä käyttöoikeudet palveluntarjoajalle. (Xiao ym. (2019).) Tutkimuksessaan Chen ym. (2014) esittivät, että melkein 60 prosentissa mobiilisovelluksissa OAuth-protokollaa toteutettiin väärin, ja Sun ja Beznosov (2012) mainitsevat että useiden toimittajien OAuth-kertakirjautumisjärjestelmät (Single-Sign-On, SSO) sisältävät kriittisiä haavoittuvuuksia.

Ylioikeutettuja hyökkäyksiä tapahtuu, kun sovellukselle tai laitteelle myönnetään käyttöoikeudet, jotka ovat vahvempia tai enemmän kuin se tarvitsee. Ylioikeuksista johtuvia ongelmia on havaittu tyypillisissä valtuutusjärjestelmissä, muun muassa älykotien alustajärjestelmissä (Fernandes, Jung ja Prakash 2016), jopa kolmanneksessa Android-sovelluksista (Felt ym. 2011) ja Ho ym. (2016) mukaan kaikissa kaupasta saatavissa älylukoissa.

3.3.5 Välimieshyökkäys

Välimieshyökkäyksessä hyökkääjä kaappaa kahden solmun välisen viestinnän ja asettuu välityspalvelimen rooliin. Reunalaskennassa yleisemmin hyökkäys kohdistetaan esineiden internetin laitteen ja siihen liittyvän toimijan välillä. (Kuzlu, Fair ja Guler (2021).) Välimieshyökkäys on Aliyu, Sheltami ja Shakshuki (2018) mukaan yleensä erittäin vaikea havaita. Hyökkääjä on myös erittäin motivoitunut, koska useasti reunalaskennassa käsitellään henkilökohtaisia tietoja, kuten terveys tai ajoneuvon määränpää.

Resurssirajoitteisina ja standarditoteutuksien puuttuessa laitteet ovat alttiita hyökkäyksille. Myös erilaiset pienikokoisiksi, halvoiksi ja energiatehokkaiksi suunnitellut langattomat teknologiat, kuten yleisesti reunalaiteissa käytetty Bluetooth Low Energy (BLE), ovat alttiita välimieshyökkäyksille. (Aliyu, Sheltami ja Shakshuki (2018) ja Kuzlu, Fair ja Guler (2021).)

Välimieshyökkäyksissä on kaksi yleistä muotoa: 1) kysely ja 2) suora yhteys. Kyselyssä laite on jatkuvassa yhteydessä pilveen, esimerkiksi tarkistaakseen laiteohjelmistopäivityksiä. Hyökkääjät voivat ohjata verkkoliikennettä uudelleen muuttamalla nimipalvelinasetuksia (Domain Name System, DNS), käyttämällä hyväkseen osoitteenselvitysprotokollaa (Address Resolution Protocol, ARP), sieppaamalla liikennettä käyttämällä itse allekirjoitettuja varmenteita tai työkaluja kuten SSL-strip. Suoran yhteyden hyökkäyksessä hyökkääjä paikantaa laitteita paikallisverkossa etsimällä kaikista osoitteista tiettyä porttia, eli käyttää samaa tekniikkaa kuin reunan sovellukset kommunikoidessaan vaikkapa keskittimen kanssa. (Kuzlu, Fair ja Guler (2021).)

3.3.6 Huonojen tietojen lisäys

Kun hyökkääjällä on pääsy joihinkin tai kaikkiin reunaverkon laitteisiin, esimerkiksi välimieshyökkäyksen kautta, huonojen tietojen lisäyshyökkäys on helppo suorittaa. Siinä hyökkääjä muuttaa epäilyksiä välttääkseen sensoreiden mittaustietoja vain hieman, ja välittää muutetut tiedot eteenpäin käsiteltäväksi, esimerkiksi algoritmille, joka yrittää tehdä ennusteita vastaanottamiensa tietojen perusteella, tai muuten käyttää dataa johtopäätösten tekemiseen. Pienetkin muutokset, vaikkapa ennakoivien huoltojärjestelmien tiedoissa, riittävät vääristämään ennusteita ja vaikkapa viivästyttämään kriittistä huoltoa. (Kuzlu, Fair ja Guler (2021).) Tehtaiden, sähköverkkojen, autojen tai lentokoneiden vikaantumiset voivat aiheuttaa kalliita suunnittelemattomia viiveitä, vaarantaa yhteiskunnan huoltovarmuuden tai ihmishenkien menetyksiä.

4 Reunalaskennan turvallisuushaasteiden ratkaisuja

Reunalaskennan ominaisuuksien, kuten monimuotoisen hajautetun arkkitehtuurin, massiivisen tiedonkäsittelyn, rinnakkaislaskennan, sijaintitietoisuuden ja liikkuvuustuen vaatimuksien vuoksi perinteiset pilvipalvelujen tietoturva- ja yksityisyydensuojamekanismit eivät sovellu reunalaskennan tietoturvan suojaamiseen. Reunalaskenta on hajautettu vuorovaikutteinen laskentajärjestelmä, jossa on useita luottamusalueita ja niissä useita oikeudellisia toimijoita. Todennusmekanismi ei vaadi vain identiteetin vahvistamista jokaiselle toimijalle yhdessä luottamustoimialueessa, vaan vaatii myös kaikkien toimijoiden keskinäisen todennuksen eri luottamusalueilla. Lisäksi joillakin resurssirajoitteisilla päätelaitteilla on mahdotonta tallentaa suurta määrää tietoa, tai suorittaa erittäin monimutkaisia suojausalgoritmeja.

Zhang ym. (2018) toteavat reunalaskennan tietoturvan ja yksityisyyden säilyttämisen kohtaavan lähinnä seuraavat uudet vaatimukset:

- **Kevyt ja hienorakeinen**: Tietojen salausmenetelmien on oltava laskennallisesti keveitä, samalla kun tiedonjakojärjestelmien on oltava tarpeeksi hienorakeisia ja perustua useisiin valtuutettuihin osapuoliin.
- **Hajautettu pääsynhallinta**: Usean lähteen monimuotoisen tiedon levityksen ohjauksen ja tiedonsuojauksen hallinnan on toimittava hajautetussa laskennassa.
- **Resurssit rajoittavat**: Tietoturvallisen yhteistoiminnan laajojen reunapalvelujen ja resurssirajoitteisten reunalaitteiden välillä on toimittava.
- **Tehokas yksityisyyden säilyttäminen**: Eri reunapalvelut ja reunalaskentamallit tarvitsevat tehokkaat yksityisyydensuojamekanismit.

Haasteista johtuen Alwakeel (2021) puolestaan listaa useita reunalaskentaan liittyviä tietosuojaongelmia, kuten:

- Heikot tietoturvatekniikat ja -algoritmit järjestelmän suojaamiseksi, esimerkiksi toimijoiden lisäämisessä.
- Toimijoiden väliset turvattomat viestintäistunnot.
- Tietojen varmuuskopiointi ja palautus järjestelmäkatkojen varalle on vaikea järjestää.
- Järjestelmään ei ole toteutettu erityistä päivityksen vastaanotto- ja toteutusmallia.

- Verkkonäkyvyyden puute.
- Käyttäjien tiedonkeruu ei ole valikoivaa.

Seuraavissa luvuissa kuvataan joitain vastatoimia reunalaskennan turvallisuus- ja tietosuojahyökkäysten käsittelemiseksi ja niiden aiheuttaman riskin vähentämiseksi.

4.1 Yleisimpien hyökkäystyyppien estoratkaisuja

4.1.1 Palvelunestohyökkäys

Kuormitukseen perustuvien hyökkäysten perimmäiset mahdollistajat ovat protokollatason suunnitteluvirheet tai haavoittuvuudet verkkoviestintäprotokollien sisällä. Nollapäivähyökkäyksissä perusmahdollistaja on kooditason haavoittuvuuksissa, jotka voivat johtaa muistihäiriöihin ja vikaantumisiin. Vastaavasti nykyiset puolustusratkaisut kuormitushyökkäyksiä vastaan noudattavat pääasiassa havaitsemissuodatinfilosofiaa, kun taas nollapäivähyökkäyksiä vastaan suunnatut ratkaisut keskittyvät pääasiassa kooditason haavoittuvuuksien tunnistamiseen. Ometov ym. (2022) tiivistävät puolustusratkaisut reitityssuojauksen käyttöönottoon ja solmujen toiminnan tarkkailuun.

Kuormitukseen perustuvan hyökkäyksen havaitseminen luokitellaan pääasiassa kahteen luokkaan: pakettikohtaiseen ja tilastopohjaiseen havaitsemiseen.

Kuormituksen perustuvat palvelunestohyökkäykset käynnistetään pääasiassa lähettämällä valtava määrä haitallisia tai väärin muotoiltuja verkkopaketteja, jolloin nämä paketit on havaittava ja suodatettava. Sen tekeminen ei kuitenkaan ole yksinkertaista eikä helppoa, ja hyökkääjillä on käytettävissään kehittyneitä tekniikoita, joilla paketteja voidaan muokata, kuten väärennetyt IP/MAC-osoitteet (Internet Protocol/Media Access Control), erilaiset HTTP-otsikot ja -agentit, ja työkalut kuten hping3. Ratkaisuiksi on ehdotettu pakettisuodatusmekanismien integrointia ruuhkanhallintakehyksiin, samasta polusta tulevien samalla tunnisteella olevien pakettien pudottamista ennen kuin ne saapuvat reunapalvelimille, ja negatiivista valinta-algoritmia, jossa palvelin ylläpitää joukkoa laillisista osoitteista. Tämä edellyttää kuitenkin asiakkaan kertovan osoitteiden muutoksista palvelimelle, eikä siten ole kovin tehokasta. (Xiao ym. (2019).)

Tilastopohjainen havainnointi ei vaadi pakettikohtaisia tietoja, kuten paketin tunnistetta ja IP/MAC-osoitteita, havaitakseen hyökkäyksen. Nykyiset tilastopohjaiset tunnistusratkaisut käyttävät joko pakettientropia- tai koneoppimistyökaluja. Entropiaan perustuvat mekanismit vaativat manuaalisia toimia, ja ovat vaikeuksissa, jos hyökkäysliikenne on salattua. Havaitsemisen automatisoimiseksi tutkijat ovat käyttäneet kone- ja syväoppimistekniikoita (Livadas ym. 2006; Zolotukhin ym. 2016). Tekniikat ovat alttiita ylisovitukselle, ja toimivat siis vaihtelevalla teholla erilaisten hyökkäysten tapahtuessa. Tilastopohjaiset tekniikat tarvitsevat suuren määrän palvelunestoliikennettä entropialaskentaa tai koulutusta varten, ja toimivat siis vasta kun liikenne jo vahingoittaa reunan toimijoita. (Xiao ym. (2019) ja Alwakeel (2021).)

Alwakeel (2021) ehdottaa tunkeutumisen havainnointijärjestelmän (Intrusion Detection System, IDS) käyttöä kuormitushyökkäyksiä vastaan, hajautetussa reunajärjestelmässä jopa erilaisten havainnointijärjestelmien koordinointijärjestelmän käyttöä, joka kuitenkin luo haasteita viiveiden hallinnassa. Viiveen hallintaan Samy, Yu ja Zhang (2020) esittelevät kevytrakenteisen hajautetun syväoppimisjärjestelmän.

Nollapäivähyökkäysten torjunta pohjautuu yleensä muistivuotojen havaitsemiseen, ja vaativat alkuperäisen lähdekoodin saatavuutta. Reunalaitteilla tämä ei yleensä ole mahdollista. Syväoppimismallien, kuten takaisinkytkettyjen hermoverkkojen (Recurrent Neural Networks, RNN), graafista dataa hyödyntävien hermoverkkojen (Graph Neural Networks, GNN) ja syvän luonnollisen kielen käsittelyn (Natural Language Processing, NLP) avulla on kuitenkin onnistuttu tunnistamaan haavoittuvuuksia ilman lähdekoodia pelkästään laiteohjelmistosta. Salauksen ja virhejäljityksen eston takia laiteohjelmistotkaan eivät yleensä ole saatavilla. Muut ehdotetut ratkaisut eivät yleensä skaalaudu, vaatiessaan jatkuvaa ihmisten välistä vuorovaikutusta, kuluttavat rajallisia laskentaresursseja suojatessaan muistia, tai vaativat ohjelmisto-ohjattavaa verkkoa (software-defined networking, SDN) käyttävää palomuuria. (Xiao ym. (2019) ja Alwakeel (2021).)

Lohkoketjun käyttö tuo Alwakeel (2021) mukaan reunalaskentaverkon turvaamiseen erinomaisia suojaominaisuuksia, kuten:

- vähentää yksittäisen pisteen epäonnistumista,

- mahdollistaa verkkotapahtuman erittäin turvallisella salausalgoritmilla,
- pystyy seuraamaan toimijan tilaa tehokkaasti, ja
- lohkoketjuun ei voida puuttua.

Kuormitushyökkäysten lisäksi lohkoketjujen käyttö toimii muissakin hyökkäyksissä, kuten välimies- ja huonojen tietojen lisäyshyökkäyksessä.

4.1.2 Sivukanavahyökkäys

Sivukanavahyökkäysten perimmäinen mahdollistaja on piilossa oleva korrelaatio suojattavien arkaluonteisten tietojen ja julkisesti saatavilla olevien sivukanavatietojen välillä. Korrelaatio voi olla hyvin monimutkainen ja vaikeasti tunnistettavissa. Sivukanavahyökkäyksiä vastaan voidaan suojautua kahdella tavalla: 1) rajoittamalla pääsyä sivukanavan tietoihin ja 2) suojaamalla arkaluonteisia tietoja päätelmähyökkäyksiltä. Rajoittamisessa on kokeiltu lähdekooditasolla sivukanavien hämärtämistä (obfuscation) ja laitteistotason suojausta. Tutkijoiden mukaan ei ole olemassa toimivaa puolustusmekanismia, joka voisi rajoittaa pääsyä hallitsemattomiin sivukanaviin. Täten arkaluonteisten tietojen suojaaminen jää ainoaksi vaihtoehdoksi. (Xiao ym. (2019) ja Mosenia ja Jha (2017).)

Häirintämalleista (perturbaatio) tunnetuin algoritmi arkaluontoisten tietojen suojaamiseksi päätelmähyökkäyksiltä on k-anonymiteetti, joka tarkoittaa anonymisointia muodostamalla k-määrästä keskenään samankaltaisista yksiköistä ryhmiä. K-anonomiteetti ja sen seuraajat tarjoavat kohtuullisen yksityisyyden suojan, mutta niillä ei ole vankkaa teoreettista perustaa, eivätkä ne estä päättelemästä arkaluonteista arvoa, jos kaikki ryhmän yksiköt saavat tietyssä muuttujassa saman arkaluonteisen arvon. Sivukanavien tietosuojassa käytetty differentiaalinen yksityisyys (differential privacy) on ainoa malli, jolla on tiukat matemaattiset todisteet. Differentiaalinen yksityisyys tarkoittaa matemaattisen kohinan lisäämistä dataan, jolloin yksittäisen yksikön erottaminen datajoukosta vaikeutuu. (Xiao ym. (2019), Tietoarkisto (2022), Google (2022b) ja Mosenia ja Jha (2017).) Sivukanavahyökkäyksiin toimivana mallina Alwarafy ym. (2021) mainitsevat myös tiedonsiirron mallin poistamista lisäämällä tarkoituksella väärennettyjä paketteja, jolloin liikennemalli muuttuu. Alwarafy ym. (2021) ja Sengupta, Ruj ja Das Bit (2020) ehdottavat käytettäväksi sivusignaalianalyysiä ja toimijoi-

den järjestelmäpiirien muuttamista. Sivusignaalianalyysissä havainnoidaan reunatoimijoissa epätavallista toimintaa, kuten lämmön, suoritusajan tai virrankulutuksen merkittävää kasvua. Järjestelmäpiirien muokkaamisessa voidaan esimerkiksi upottaa PUF-funktio (Physically Unclonable Function) piirilaitteistoon, mikä mahdollistaa laitteen yksilöllisen tunnistamisen ja laitteen muutosten havaitsemisen.

Suojaamismallit voivat tehokkaasti estää päättelemästä arkaluontoisia tietoja, mutta voivat samalla uhrata tiedon hyödyllisyyden. Rajoitusratkaisuja, kuten lähdekooditason hämärtäminen ja laitteistosuojaus, on mahdotonta soveltaa jokaiseen sivukanavatietoon. Valittavasti monet olemassa olevista ratkaisuista ovat myös itse alttiita sivukanavahyökkäyksille. (Xiao ym. (2019).) Salauksen (kuten Lightweight Encryption Algorithm, LEA) käyttöä on ehdotettu mallien tukena, joka kuitenkin johtaa suorituskykyhaasteeseen (Sengupta, Ruj ja Das Bit 2020). Salauksen tunnettuihin sivukanavahaasteisiin Lu ym. (2021) ehdottavat kaksoiskopiointijärjestelmää, joka tutkimuksen mukaan kestää sivukanavahyökkäyksiä.

4.1.3 Haittaohjelmien lisäyshyökkäys

Xiao ym. (2019) mukaan reunapalvelimien haittaohjelmien lisäysten perimmäiset mahdollistajat ovat protokollatason suunnitteluvirheissä, suunnittelijoiden keskittyessä pääasiassa hyödyllisyyteen ja pitäessä turvallisuutta merkityksettömänä, sekä toteutuksen puutteet. Toteutustason puutteisiin on kaksi pääasiallista syytä: 1) kehittäjät voivat ymmärtää protokollan perusteet väärin ja 2) protokollan siirtäminen muista alustoista reunalaskenta-alustaan voi aiheuttaa yhteensovitusongelmia. Reunalaitteiden haittaohjelmien lisäyksissä mahdollistajat puolestaan ovat kooditason suunnitteluvirheissä sekä karkearakeisten käyttöoikeuksien valvontamallien käytössä. Palvelimissa lisäyksiä vastaan suojaudutaan pääasiassa havaitsemissuodattimilla, ja laitteissa lisäyksiä vastaan suunnatut suojaukset keskittyvät pääasiassa kooditason analyyseihin haitallisen toiminnan havaitsemiseksi ja hienorakeiseen kulunvalvontaan. (Xiao ym. (2019).) Havaitsemistekniikoista Ometov ym. (2022) mainitsevat erityisesti allekirjoitukseen ja käyttäytymiseen perustuvat tunnistukset sekä Mirai-botnet tunnistimen.

Puolustukset kaikkia reunapalvelimiin kohdistuvia neljää tyyppiä (kyselykielen lisäys, verk-

kosivustojen väliset komennot, verkkosivustojen välisten pyyntöjen väärennös, palvelinpyynnön väärennös ja merkintäkielen allekirjoituskääreet) ovat samanlaisia. Ne luokitellaan Rana (2011) mukaan havaitsemiseen ja ennaltaehkäisyyn. Havaitsemiseen keskittyvät tekniikat käyttävät periaatteessa koodintarkistusta erilaisilla menetelmillä, kuten staattinen analyysi, dynaaminen virheenkorjaus ja black box-testaus. Ehkäisyyn keskittyvät tekniikat pyrkivät estämään laittomien SQL-kyselyjen suorittamisen, esimerkiksi käyttämällä välityspalvelimen suodattimia ja käskysarjan satunnaistamista (Instruction-Set Randomization, ISR). (Xiao ym. (2019) ja Ometov ym. (2022).) Tekniikat kuten syöttökyselyiden vertaaminen ohjelmoijan suunnittelemiin tai SQL-kyselyn attribuuttien arvojen poisto ja lisäanalyysi ennen suorittamista vaativat aluksi manuaalista työtä. Koneoppimisen ja syväoppimisen avulla onkin havaittu tarkkuuden paranevan lisäyshyökkäysten havaitsemisessa. (Xiao ym. (2019).)

Verkkosivustojen välisten komentojen puolustusjärjestelmiin kuuluvat muiden muassa kovakoodattujen sääntöjen manuaalinen käyttöönotto ja käskysarjojen satunnaistaminen. Pyyntöjen väärennösten esto pohjautuu ensisijaisesti viittausotsikkojen tarkistuksiin, asiakkaiden tunnistetietojen upottamiseen pyyntöihin tai verkkosovellusten palomuurin (Web Application Firewall, WAF) toimintaan. Allekirjoituskääreitä vastaan toimitaan tarkistamalla pyyntö W3C XML skeemaa vastaan ja tarkistamalla noodien määrät ja sijainnit. (Xiao ym. (2019).)

Reunalaitteisiin kohdistetuissa lisäyshyökkäyksissä suurin uhka tulee laiteohjelmiston muutoshyökkäyksistä. Käskysarjojen satunnaistamisen tapaisia tekniikoita kuten osoitetilan asettelun satunnaistamista (Address Space Layout Randomization, ASLR) ja automaattista binäärirakenteen satunnaistamista (Autonomic Binary Structure Randomization, ABSR), on ehdotettu. Ne, kuten myös lohkoketjupohjaiset reunalaitteiden päivitysmenetelmät, eivät ole helppoja toteuttaa ja voivat olla laskennallisesti liian vaativia reunalaitteille. Erillinen muistinsuojausyksikkö (Memory Protection Unit, MPU) ei puolestaan sovi kaikkiin suoritinarkkitehtuureihin. (Xiao ym. (2019).) Erilaisia resurssitehokkaita todennusmekanismeja ja hajautettuja arkkitehtuureita on Alwarafy ym. (2021) mukaan kylläkin ehdotettu laskentatarpeen vähentämiseksi. Sengupta, Ruj ja Das Bit (2020) mainitsevat PUF-funktion käytön (Physically Unclonable Function) perustuvan todennusprotokollan, jonka väärentäminen kloonaamalla on mahdotonta.

Mobiililaitteisiin kohdistuvat haittaohjelmahyökkäykset käyttävät hyväkseen mobiilikäyttö-

järjestelmien suunnitteluvirheitä ja haitallisia kirjastoja. Näitä on mahdollista tunnistaa staattisilla analyysimenetelmillä, esimerkiksi kuten Wu ym. (2012) esittävät. Tutkijoiden mukaan osaan uhkista ei ole käytännöllisiä torjuntaratkaisuja, ellei Android-ytimen suojausta paranneta tai Android-käyttöjärjestelmää suunnitella uudelleen. (Xiao ym. (2019).)

4.1.4 Todennus- ja valtuutushyökkäys

Sanakirjahyökkäysten perimmäinen mahdollistaja on heikkojen valtuustietojen käyttö todennusprotokollassa, ja kolmen muun (todennusprotokolla, valtuutusprotokolla ja ylioikeus) hyökkäystyypin mahdollistajina ovat protokollatason suunnitteluvirheet tai toteutustason puutteet. Suojaus sanakirjahyökkäyksiä vastaan keskittyy pääasiassa vahvemman todennuskerroksen lisäämiseen tai salasanan vahvistusprosessien tiukentamiseen. Suojaukset kolmea muuta hyökkäystyyppiä vastaan perustuvat pääasiassa nykyisten protokollien paikkaamiseen ja vahvistamiseen, tai kooditason analyysien tekemiseen. (Xiao ym. (2019).)

Sanakirjahyökkäyksen kohdalla ajatellaan, että pelkkä monimutkaisten salasanojen pakottaminen todennusta varten voi ratkaista ongelman. Tämä ei kuitenkaan välttämättä ole mahdollista ainakin kolmesta syystä. Ensinnäkin reunatoimijoiden rajallisen laskentatehon vuoksi monimutkaisten salasanojen käyttö voi lisätä laskennan kuormitusta. Toiseksi reunalaskennassa voi olla paljon enemmän tilaajia eli reunalaitteita. Monimutkaisten salasanojen käyttö lisää tallennustaakkaa. Kolmanneksi tunnistetietojen tallentaminen reunalaitteisiin ei ole turvallista, koska ne ovat alttiimpia salasanavuodoille hauraan tietoturvan takia. Moni tutkimus ehdottaakin siksi yhden todennuskerroksen lisäämistä, eli kaksivaiheista tunnistusta. Tunnetuimmat kaksivaiheiset todennusmekanismit käyttävät toisena vahvistajana erilaisia ominaisuuksia, kuten sormenjälkiä (Jin, Ling ja Goh 2004), kasvontunnistusta (Schroff, Kalenichenko ja Philbin 2015), tekstiviestejä (Aloul, Zahidi ja El-Hajj 2009) tai jopa ympäristön ääntä (Karapanos ym. 2015). Useimmat vaativat ihmisen vuorovaikutusta, ja ovat siten reunajärjestelmissä vaikeasti käytettävissä. Menetelmät ovat osoittautuneet käytännössä myös epävarmoiksi, ja jokaiseen yllämainittuun todennusmekanismiin on olemassa murtoratkaisu, kuten mobiilitroijalainen tai väsytyshyökkäys. (Xiao ym. (2019).)

Todennusprotokollien haavoittuvuuksia hyödyntäviä hyökkäyksiä vastaan pyritään paranta-

maan tietoliikenneprotokollien turvallisuutta tai suojaamaan kryptografiset toteutukset. Tällöin muutetaan esimerkiksi WPA/WPA2 avainten vaihtoprosessia käyttämällä julkisten avainten kryptografiaa, tai tutkitaan kuten Bhargavan, Blanchet ja Kobeissi (2017) tunnettujen TLS 1.2 hyökkäyksien toteutuksia TLS 1.3 vastaan. Vaihtoprosessi ei kuitenkaan suojaa avainten uudelleenkäytöltä, ja toteutusten tutkiminen ei vastaavasti onnistu reaaliaikaisesti. (Xiao ym. (2019).)

Valtuutusprotokollien haavoittuvuuksista tunnetuimpia ovat OAuth-protokollan toteutusheikkoudet, vaikka OAuth 2.0 onkin teoriassa turvallinen. Ratkaisuiksi on ehdotettu staattista koodianalyysiä, erilaisen OAuth Manager ohjelmistokehyksen käyttöä (Shehab ja Mohsen 2014) tai erilaista OAuth-protokollatoteutusta reunatoimijoiden tarpeisiin (Cirani ym. 2015).

Ylioikeutettujen hyökkäyksien torjuntaan on ehdotettu muun muassa neuroverkkopohjaisia menetelmiä ja erilaisten sovellusten käyttöä sovelluksen toteutuksen ja sen kuvauksen välisten epäjohdonmukaisuuksien tarkistamiseksi. Kaikki nämä tarvitsevat valtuutuksen ja pääsyn lähdekoodiin. Sovelluksen historialliseen käyttäytymiseen pohjautuvat menetelmät puolestaan vaativat pitkäkestoisen seurannan ja hienovaraisen tilannejaottelun, ja ovat siten vaikeita toteuttaa käytännössä. (Xiao ym. (2019).) Mobiilijärjestelmien suojautuminen pohjautuu pitkälti erilaisiin hiekkalaatikkototeutuksiin, esimerkiksi kuten Fernandes ym. (2016) on esittänyt erityisesti esineiden internetin käyttöön.

Jan ym. (2019) ehdottavat artikkelissaan toimijoiden keskinäiseksi todennusjärjestelmäksi hyötykuormaan perustuvaa salausjärjestelmää, joka käyttää CoAP-protokollan (Constrained Application Protocol) kevyitä ominaisuuksia ja nelisuuntaista kättelymekanismia osallistujien henkilöllisyyden tarkistamiseen.

4.1.5 Välimieshyökkäys

Aliyu, Sheltami ja Shakshuki (2018) mukaan reunalaskennassa välimieshyökkäyksen taustamahdollistaja on reunatoimijoiden resurssien rajoitteisuus, jolloin perinteisten välimieshyökkäysten havaitsemis- ja ehkäisytekniikat ovat epäkäytännöllisempiä toteuttaa kuin perinteisissä palvelimissa.

Alwakeel (2021) ehdottaa tunkeutumisen havainnointijärjestelmän (Intrusion Detection Sys-

tem, IDS) käyttöä myös välimieshyökkäyksiä vastaan, hajautetussa reunajärjestelmässä jopa erilaisten havainnointijärjestelmien koordinointijärjestelmän käyttöä, joka kuitenkin luo haasteita viiveiden hallinnassa. Myös Aliyu ym. (2021) ja Aliyu, Sheltami ja Shakshuki (2018) ehdottavat artikkeleissaan tunkeutumisen havainnointi- ja estomekanismia, jossa reunan solmut havaitsevat säännöllisin väliajoin tapahtuvalla valvonnalla verkossa tapahtuvat poikkeamat, ja eristävät kyseiset solmut reunaverkosta. Havainnointi perustuu Aliyu ym. (2021, s. 8) mukaan kolmeen tekijään: 1) muutokseen paketin sisällössä, 2) viiveessä paketin saapumisessa tai 3) paketin kulkusuunnan muuttumiseen. Aikaleimojen käytön nostavat myös Ometov ym. (2022) tutkimuksessaan esille.

Firouzi, Farahani ja Marinšek (2021) mukaan muut tekniikat pohjautuvat reunalaitteiden tiedonvälityksen turvaamiseen vahvan avaintenhallinnan ja salausalgoritmien avulla. Alwakeel (2021) ehdottaa lohkoketjun käyttöä ja Sengupta, Ruj ja Das Bit (2020) listaavat suojattuja esineiden internetin kommunikointeja, kuten suojattu MQTT (Message Queue Telemetry Transport) ja MQTT-SN (MQTT for Sensor Networks), tai toimijoiden osallistumista istuntoavaimen muodostamiseen keskusavaimen luomisen sijasta.

Kuzlu, Fair ja Guler (2021) ehdottavat yksinkertaista toimintalistaa välimieshyökkäykseltä suojautumiseen: suorita säännöllisiä ohjelmistopäivityksiä, käytä asianmukaista palomuurikokoonpanoa, käytä vahvaa salausta, vältä turvatonta WiFi-yhteyttä, tee laitteista havaitsemattomia, suorita säännöllisiä ohjelmistopäivityksiä, estä tuntemattomat laitteet, käytä kaksivaiheista todennusta ja käytä vahvoja pariliitosmenetelmiä, kuten elliptisen käyrän Diffie-Hellmanin julkisen avaimen salaustekniikkaa.

4.1.6 Huonojen tietojen lisäys

Huonojen tietojen lisäyshyökkäyksiä voidaan tehdä monella tapaa, mutta käytännöllisintä se on tehdä välimieshyökkäyksen kautta (Kuzlu, Fair ja Guler 2021). Torjuntatoimet ovat siis pitkälti samoja. Lisäksi (Kuzlu, Fair ja Guler 2021) mukaan voidaan käyttää muun muassa poikkeamien havaitsemista, kuten tietojen sanitointia, mikromalleja ja tietojen validointijoukkoja hyökkäystarkoituksen, kuten tietojoukon myrkytyksen tai algoritmimyrkytyksen, perusteella. Alwarafy ym. (2021) listaavat lisäksi reunalaskennan tutkimuksia, joissa ei käy-

tetä julkisen avaimen järjestelmiä molemminpuoliseen todennukseen, tai käytetään uudenlaista arkkitehtuuria, jossa turvatoiminnot on siirretty pois rajoitteisilta reunalaitteilta erillisiin erikoistuneisiin moduleihin ja laitteisiin.

4.2 Yhteenvetoa taustasyistä ja ehdotetuista ratkaisuista

Kuormituspohjaisten hyökkäysten perimmäisinä mahdollistajina ovat protokollatason puutteet, jotka johtuvat turvallisuuden laiminlyömisestä alkuperäisessä suunnittelussa. Kehittäjien ohjelmoidessa miljoonien koodirivien järjestelmiä nollapäivän kooditason haavoittuvuuksia on vaikea välttää. (Xiao ym. (2019).) Ongelmia ilmenee myös näiden haavoittuvuuksien estossa, kuten Microsoftin ongelma haittaohjelmien havainnointiohjelmistossa osoittaa (Paganini 2022). Tällaisia haavoittuvuuksia on vielä vaikeampi välttää reunalaskennassa, reunatoimijoiden ottaessa käyttöön vasta kehitteillä olevia järjestelmäohjelmistoja, jotka tinkivät vahvemmasta suojauksesta alhaisempien kustannusten ja paremman käyttökokemuksen eduksi. (Xiao ym. (2019).)

Haittaohjelmien lisäyshyökkäysten mahdollistajat ovat Xiao ym. (2019) mukaan reunapalvelimissa protokollatason suunnitteluvirheet, reunalaitteilla puolestaan kooditason suunnitteluvirheet ja laitetason käyttöoikeuksien hallinnassa. Nykyiset torjuntaratkaisut eivät toimi reaaliajassa, vaativat täyden pääsyn joko laiteohjelmistoon tai lähdekoodeihin, eivätkä käytännössä voi estää vaikkapa nollapäivän haavoittuvuuksista johtuvia hyökkäyksiä. Käyttöoikeuksien hallinta heikoilla allekirjoituksen varmentamiseen perustuvilla suojauksilla ovat tehottomia, eikä hienojakoisempien käyttöoikeuksien käyttöä lisäyshyökkäysten estoon ole tutkittu.

Todennus- ja valtuushyökkäyksissä perusmahdollistajat ovat sanakirjahyökkäyksissä heikkojen valtuustietojen käyttäminen ja muissa protokollatason suunnitteluvirheet tai toteutuksen heikkoudet. Näitä vastaan puolustautuminen on osoittautunut hankalaksi ehdotettujen ratkaisujen, kuten kaksivaiheisen tunnistuksen, tehottomuuden takia. (Xiao ym. (2019).)

Erilaiset pilvipalveluiden tietoturvaratkaisut eivät yleensä ole tehokkaita reunalaskennan kanssa, joten reunalaskennalle on Alwakeel (2021) ehdottanut ratkaisuja kuten:

- Samaa suojaustasoa on sovellettava kaikissa reunaverkon solmuissa asianmukaisen turvallisuusprotokollan varmistamiseksi.
- Kaikkia reunasolmuja on välttämätöntä pitää jatkuvassa tarkkailussa.
- On käytettävä uusia huippuluokan salausalgoritmeja, joiden purkaminen on erittäin monimutkaista. Nämä algoritmit koostuvat salaisesta avaimesta, joka on asianmukaisesti suojattu ja jaettu laillisen lähettäjän ja vastaanottajan välillä.
- On otettava käyttöön tunkeutumisen havaitsemisjärjestelmä poikkeavuuksien tai luvattoman käytön havainnoimiseen.
- On suoritettava käyttäjien käyttäytymisen profilointia, jolloin mikä tahansa normaalista käyttäytymisestä poikkeava toiminta auttaa määrittämään haitallisen käyttäjän läsnäolon.

5 Auto reunalaitteena

Puoli- ja täysin autonomisten ajoneuvojen markkinoiden ennustetaan olevan kasvussa, ja pelkästään Kiinassa on arvioitu olevan autonomisia autoja vuoteen 2035 mennessä noin 8,6 miljoonaa. Boston Consulting Group arvioi autonomisten ajoneuvojen saavuttavan 25 prosentin markkinaosuuden maailmanlaajuisesti vuosina 2035-2040. Cisco (2020) mukaan nopeimmin kasvava esineiden internetin sovellustyyppi on verkkoon yhdistetty auto, ja verkkoautosovellukset kasvavat nopeimmillaan 30 % vuosivauhtia vuosina 2018–2023.

Autot ovat pitkän aikavälin hyödykkeitä, ja on muistettava, että nykyisten modernien autojen sensori-, laskenta-, suojaus- ja salaustekniikat ovat vähemmän tehokkaita tulevaisuudessa (West 2016). Nykyiset autot eivät vielä täytä SAE International (2021) määritelmää tason 5 täysin automaattisesta ajamisesta, mutta mahdollistavat toiminnot joissa kuljettajalla on vastuu, mutta auto voi suorittaa itse toimenpiteitä. Tutkielmassa keskitytäänkin nykyisten autojen tason 1–3 mahdollistamiin käyttötapauksiin.

- 1-taso: Kuljettajalla on oltava auto koko ajan kontrollissa. Tukijärjestelmät ovat edistyneempiä, auto voi avustaa esimerkiksi ohjaamisessa, kiihdyttämisessä ja jarruttamisessa ajoympäristön mukaan.
- 2-taso: Osittainen automaatio. Hiukan enemmän ajotilannekohtaisia kuljettajan tukijärjestelmiä, kuten esimerkiksi tutkapohjainen vakionopeudensäädin, AutoPilot (Tesla) ja puoliautomaattinen parkkeerausavustin.
- 3-taso: Ehdollinen automaatio. Kolmostasolla kuljettaja voi halutessaan antaa auton suorittaa joitakin toimenpiteitä itse. Kuljettaja voi välillä siirtää katseensa pois liikenteestä ja antaa auton huolehtia ajosta. Auto pystyy ottamaan joissakin tilanteissa kontrollin, mutta kuljettajan on otettava jälleen ajovastuu, jos jokin järjestelmä niin hälyttää.

Autonomiset toiminnot, kuten adaptiiviset vakionopeudensäätimet, kaistavahdit, ajoneuvon sisäinen kunnonvalvonta, etähallinta ja etäpäivitykset, ovat tullet mahdollisiksi ohjelmistopohjaisten elektronisten ohjausyksiköiden (Electric Control Unit, ECU) avulla. Chowdhury ym. (2020) mukaan samalla kun ne ovat poistaneet mekaaniset ohjausominaisuudet, ovat ne

mahdollistaneet valtavat säästöt autonvalmistajille. Khatri, Shrestha ja Nam (2021) mukaan nykyaikaisissa korkean teknologian autoissa on jopa 70 ohjausyksikköä, ja 2500 elektronista signaalia vaihdetaan eri komponenttien välillä. Autonvalmistajista BMW (2020) ilmoittaa autojensa sisältävän 50–60 etäpäivitettävää laskentayksikköä, jotka mittaavat ja säätelevät kaikkea navigointijärjestelmästä ohjauspyörään. Pham ja Xiong (2021) mukaan autojen sensoriverkot koostuvat esimerkiksi laserista, tutkasta, kamerasta, paikannusjärjestelmistä (kuten Global Positioning System, GPS), valotutkasta (light detection and ranging, LiDaR) ja niiden yhteysmekanismeista, kuten matkapuhelinyhteydestä, Bluetoothista, langattomasta lähiverkosta (WiFi) ja autokäyttöön erikoistuneesta kommunikaatioteknologiasta (IEEE 802.11p Wireless Access in Vehicular Environments, WAVE). Itseajava auto tuottaa Puliafito ym. (2019) mukaan tietoa jopa yhden gigatavun sekunnissa, samalla kun liikenneturvallisuus ja itsenäiset ajopalvelut edellyttävät alle 50 millisekunnin viiveitä. Nykyaikainen auto onkin varsin monipuolinen reunatoimija, joka tekniikan kehittymisen myötä tulee viestimään ja vastaanottamaan entistä enemmän tietoa muiden reuna- ja pilvitoimijoiden kanssa, samalla kun ajosuorite tulee siirtymään muun muassa turvallisuus- ja mukavuussyistä enemmän kuljettajalta ajoneuvolle. Reunatoimijana auto tulee myös mahdollistamaan valmistajille uudenlaisia liiketoimintamalleja, esimerkiksi teiden kuntoon, säätilaan, liikennetilanteeseen tai käyttäjän toimintaan liittyvien tietojen muodossa.

Itseohjautuvien ajoneuvojen ajotestien alkamisesta lähtien ajoneuvojen eri yksiköitä vastaan on tehty hyökkäyksiä, ja Chowdhury ym. (2020) mainitsevat niitä raportoidun noin 126 tapausta. Chattopadhyay, Lam ja Tavva (2021) puolestaan sanovat kyberhyökkäysten määrän 6-kertaistuneen vuodesta 2010 vuoteen 2018, ja raportoitujen tapausten määrän olleen 170 joista 60 pelkästään vuonna 2018. Hyökkäyksistä yli 91 % oli langattomia, ja 21 % pitkän kantaman hyökkäyksiä. Esimerkkeinä voidaan mainita vaikkapa seuraavat:

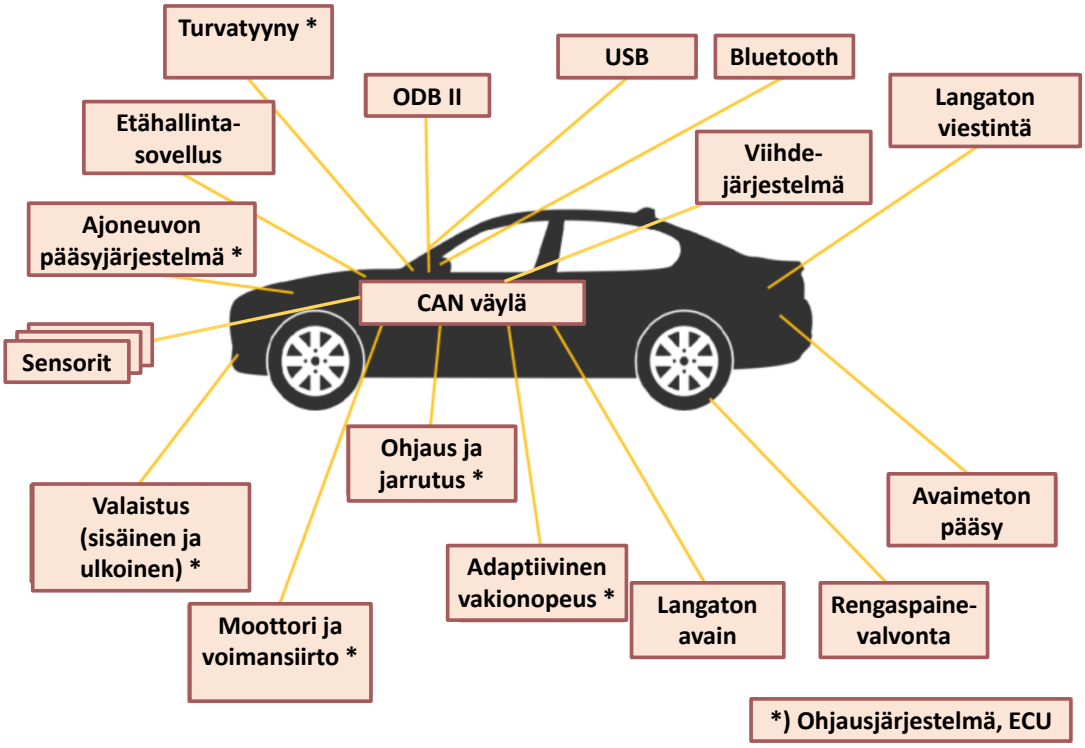
- Miller ja Valasek (2015) ottivat valtatiellä ajaneen auton (Jeep) hallintaansa etänä hyödyntäen auton viihdejärjestelmää, eikä kuljettajalla ollut valtaa ohjauspyörän tai polkimien hallintaan.
- Jagielski ym. (2018) hyökkäsivät ajoneuvon (Tesla) valotutkaa vastaan, jolloin se ei kyennyt havaitsemaan edessä olevaa pakettiautoa, mikä johti ajoneuvojen törmäykseen.

- Zaabi, Yeun ja Damiani (2019) kontrolloivat sähköauton (Nissan Leaf) akkua hyödyntäen ajoneuvoa säätelevän Nissan Connect -mobiilisovelluksen haavoittuvuuksia.

Selittämättömät liikenneonnettomuudet, kuten tappouhkauksen alla olleen henkilön ja henkivartijoiden kuolemaan johtanut törmäys (BBC News 2021), aiheuttavat myös spekulaatioita mahdollisista hyökkäyksistä.

5.1 Auton mahdollisia hyökkäysrajapintoja

Auton mahdollisia hyökkäysrajapintoja ovat listanneet (Chattopadhyay, Lam ja Tavva 2021; Khatri, Shrestha ja Nam 2021) kuviossa 4. Ne voidaan jakaa kahteen tyyppiin, fyysisen liitännän tarjoaviin ja etähallittaviin.



Kuvio 4. Auton hyökkäysrajapintoja (Chattopadhyay, Lam ja Tavva 2021; Khatri, Shrestha ja Nam 2021) mukaillen.

Fyysiset rajapinnat:

- **OBD (On-Board Diagnostic)** on yhteysportti, joka löytyy versiona II melkein kaikista nykyaikaisista ajoneuvoista. Sen kautta kuka tahansa voi kerätä tietoja ajoneuvon päästöistä, ajokilometreistä, nopeudesta ja tietoja ajoneuvon osista, myös reaaliaikaisesti. OBD tarjoaa myös tavan hankkia tietoja elektronisista ohjausyksiköistä, ja mahdollisesti muokata näihin ohjausyksiköihin upotettua ohjelmistoa. Monet valmistajat käyttävät myös OBD-portteja laiteohjelmistopäivitysten suorittamiseen. OBD-portti ei yleensä salaa tietoja tai rajoita pääsyä. Koska itse OBD-portilla ei ole etäyhteyttä, hyökkääjät tarvitsevat fyysisen pääsyn OBD-porttiin suorittaakseen nämä hyökkäykset. Jotkut OBD-porttiin kytketyt laitteet voivat siirtää tietoja langallisten tai langattomien yhteyksien kautta. (Pham ja Xiong (2021).) Näitä yleiskäyttöisiä langallisia ja langattomia OBD-vikakoodinlukijoita on hyvin tarjolla. Vikakoodien luvun lisäksi esimerkiksi Achakey (2022) tarjoaa autoon liitettävää OBD-laitetta ja Bluetoothin avulla kommunikoivaa mobiilisovellusta, jonka avulla auton ovia voidaan kontrolloida ilman avainta.
- **CAN-väylä (Controller Area Network (CAN) bus)** on vanha järjestelmä, jota on käytetty keskusverkkona ohjausjärjestelmien (ECU) välillä. Valmistajat ovat käyttäneet CAN-väylää laajasti sen yksinkertaisuuden ja alhaisten johdotuskustannusten takia. Ohjausjärjestelmien reaaliaikaiset viestit, muun muassa moottorin, jarrujen, ohjauksen, turvatyynyjen ja muiden turvajärjestelmien ohjaukseen, lähetetään kaikkiin verkon solmuihin, eivätkä paketit sisällä todennus- tai lähteen tunnistuskenttää. Yksikin vaarantunut solmu (ohjausjärjestelmä) voi kerätä kaiken siirrettävän tiedon, lähettää haitallisia tietoja muille solmuille tai lähettämällä korkean prioriteetin viestejä estää muiden solmujen tiedonkäsittelyn. CAN-väylän ollessa yleisin myös muita vastaavia kommunikointikanavia, kuten Local Interconnect Network (LIN), FlexRay ja autojen Ethernet, on käytössä. (Chowdhury ym. (2020), Pham ja Xiong (2021) ja Khatri, Shrestha ja Nam (2021).) Tutkielmassa keskitytään jatkossa vain CAN-väylän käyttöön, eikä muihin kohdistuvia uhkia käsitellä.

On huomattava, että OBD-portin kautta päästään käsiksi CAN väylään, ja sitä kautta myös kaikkiin elektronisiin ohjausyksiköihin. Pham ja Xiong (2021) mukaan haitallisen itsediagnostiikkasovelluksen avulla voidaan lähettää OBD-laitteen kautta haitallisia viestejä ohjausyksiköille. Tämän lisäksi Khatri, Shrestha ja Nam (2021) mainitsevat mahdollisuuden pääs-

tä käsiksi CAN-väylään telematiikka- tai viihdejärjestelmien etäkäytöllä. Hyökkääjä ei siis välttämättä tarvitse fyysistä pääsyä OBD-porttiin tai CAN-väylään.

Etähallittavat:

- **Etähallintasovellukset**: useat autovalmistajat, kuten esimerkkeinä KIA (2022), Mercedes Benz (2022), Volvo (2022c) ja Volkswagen (2022a) tarjoavat ajoneuvojen käyttäjille mobiileja etähallintasovelluksia. Niiden avulla nähdään muun muassa auton perustietoja, kuten polttoaineen määrä, ajetut kilometrit ja huollontarve, voidaan tarkastaa auton sijainti tai kerätä automaattista ajopäiväkirjaa, sekä kontrolloida lukkoja, lisälämmitintä ja moottoria. Sovelluksilla on siis pääsy auton ohjausyksiköihin yleensä CAN-väylän kautta.
- **Sensorit**: Nykyaikainen auto on varustettu monilla sensorijärjestelmillä ajoneuvon tilan seuraamiseksi. Yleisimmin mainitaan paikannusjärjestemät (GPS, GNSS), kamerat, asento- ja paineanturit sekä erilaiset ympäristön havainnointijärjestelmät kuten laserit, tutkat ja valotutkat. Näitä voidaan häiritä monin tavoin, esimerkiksi lähettämällä voimakkaampaa haitallista signaalia, jolloin auto voi olla havaitsematta estettä, jarruttaa ja väistää kuvitteellista estettä, tai vaikkapa pysähtyä rengaspainejärjestelmän hälyttäessä tyhjentyneestä renkaasta. (Chattopadhyay, Lam ja Tavva (2021), Chowdhury ym. (2020) ja Pham ja Xiong (2021).)
- **Ohjausyksiköt**: Elektroniset ohjausyksiköt ohjaavat muita ajoneuvon osajärjestelmiä. Kaikissa nykyaikaisissa ajoneuvoissa käytetään ohjausyksikköjä ajoneuvon toimintojen ohjaamiseen hankkimalla elektronisia signaaleja muista komponenteista sekä käsittelemällä ja lähettämällä ohjaussignaaleja. Näitä ohjausyksikköjä ovat muun muassa jarrujen-, moottorin-, rengaspaineen valvonnan ja inertian mittausyksiköt. Ohjausyksiköt ja ohjelmistot ovat yleensä päivitettävissä langattomasti, esimerkiksi kuten BMW ja Volkswagen ovat ilmoittaneet. (Pham ja Xiong (2021), BMW (2020) ja Volkswagen (2022b).)
- **Telematiikka- ja viihdejärjestelmät**: Hyökkääjät vaarantavat telemaattiset ohjausyksiköt niiden liitäntämekanismien tai langattomien ohjelmistopäivitysten kautta. Ohjausyksiköt tai niiden pääsy CAN-väylään avaa hyökkääjille keinon tietojen varastamiseen ja ajoneuvon haltuunottoon. (Pham ja Xiong (2021) ja Khatri, Shrestha ja

Nam (2021).) Autovalmistajista esimerkiksi Volvo on tarjonnut sovellusten asentamista viihdejärjestelmiinsä, ja tarjoaa jatkossa autoissaan Android käyttöjärjestelmää (Volvo 2022a, 2022b).

5.2 Auton tyypillisimpiä käyttötapauksia

Autokauppa Kamuxin teettämän tutkimuksen mukaan suomalaisten tärkeimmät auton käyttötarkoitukset ovat ostoksilla käynnit, muut asioiden hoidot, ajo työpaikan ja kodin välillä, vierailut sukulaisten ja ystävien luona sekä mökkimatkat (Iltasanomat 2021). Ajot kohdistuvat siis pääasiassa vakiintuneisiin kohteisiin, ja ajosuorite kattaa monenlaiset ympäristöt moottoriteistä mökkipoluille. Minkälaisia uhkia tällaiseen autoiluun voi kohdistua?

5.3 Riskikartoitus

Riskikartoituksessa kerätään tunnistettuja tietosuojariskejä kaikista tietoturvan osa-alueista, mutta riskejä ei vielä arvioida. Tutkielman riskikartoitukseen käytetään luvussa 3.2 esiteltyä Euroopan unionin verkko- ja tietoturvaviraston käyttämää kategorisointia, jonka jokaiseen kohtaa on tunnistettu yksi esimerkkitapaus. Esimerkkitapauksia on helppo listata kattavammin, mutta tutkielmassa listaa on rajattu yleispäteviin esimerkkeihin lähinnä yksityishenkilön näkökulmasta.

1. Ikävä toiminta / väärinkäytökset

    (a) Kohdistetulla hyökkäyksellä voidaan kerätä pitkän ajan kuluessa vaikkapa viihdejärjestelmän kautta kaikki ajoneuvossa käydyt keskustelut tai paikannustiedot.
    (b) Palvelunestohyökkäyksellä CAN-väylässä tai yksittäiseen ohjausyksikköön voidaan ylikuormittaa auton tietojen käsittelyjärjestelmä.
    (c) Kaapattu sensori (esimerkiksi GPS, kamera, tutka, asento- tai painetunnistin) tai ohjainlaite voidaan saada lähettämään väärennettyä tietoa.
    (d) Käyttäjän yksityisyys vaarannetaan etähallintasovelluksen tai auton telematiikan lähettämien tietojen, kuten olinpaikka, ajetut reitit ja asetetut määränpäät, kaappaamisella.

(e) Viihde- ja navigointijärjestelmän tietoja voidaan muuttaa tai salata.

2. Salakuuntelu / Sieppaus / Kaappaus & Tiedon sieppaus

   (a) Välimieshyökkäyksellä CAN-väylässä toimivien ohjainlaitteiden käsittely voidaan sekoittaa.

   (b) Kommunikointiprotokollan kaappauksella vaikkapa etähallintaohjelmiston ja palvelimen välillä voidaan tarkistella siirrettäviä tietoja tai antaa toimintakomentoja.

   (c) Puhelu-, pikaviesti- ja sähköpostitiedot voidaan siepata ja mahdollisesti muuttaa viihdejärjestelmän kautta.

   (d) CAN-väylän, muun ajoneuvon sisäisen viestiväylän tai ulkoisen langattoman viestinnän kautta saadaan verkkoa tutkimalla selville kytketyt laitteet, käytetyt protokollat, avoimet portit ja sisäisesti käytetyt palvelut.

   (e) Kaappaamalla etähallintaistunto voidaan tietoja varastaa, muokata tai poistaa.

   (f) Toistamalla CAN-väylän laillisia viestejä tai lykkäämällä niiden lähetyksiä voidaan manipuloida ajoneuvon toimintaa, tai aiheuttaa ohjelmiston vikatilanne.

3. Katkot

   (a) Kaappaamalla viihdejärjestelmän tai ulkoisen viestinnän järjestelmä voidaan aiheuttaa verkkokatko ja estää viestintä.

   (b) Haittaohjelmistolla voidaan aiheuttaa laitevaurio, joko yksittäisen komponentin tai koko ajoneuvon osalta.

   (c) Järjestelmävika saadaan aikaan manipuloimalla sensoreita, hyökkäämällä CAN-väylässä tai ottamalla viihdejärjestelmän sovelluksia haltuun.

   (d) Tukipalvelujen menetys (kuten SOS-järjestelmä, liikennetiedot) voidaan aiheuttaa ottamalla haltuun ulkoiset kommunikaatioväylät.

4. Vahingot / IT-omaisuuden menetys

   (a) Arkaluontoisia tietoja, kuten henkilötiedot, vieraillut paikat, puhelut ja niiden äänitykset, voidaan kerätä tietoviihdejärjestelmästä.

5. Virheet / häiriöt

   (a) Ohjelmistovirheitä, kuten heikkoja salasanoja tai määrittelyvirheitä, voidaan hyödyntää etähallintaohjelmiston hyödyntämisessä tai OBD ja CAN-väylän toimin-

nassa.

(b) Kolmannen osapuolen virhe voi johtaa esimerkiksi virheelliseen liikennetilanteen tulkintaan ja reititykseen.

6. Katastrofit

   (a) Tieto luonnon- ja ympäristökatastrofeista voidaan estää saavuttamasta ajoneuvoa kommunikaatiojärjestelmien tai viihdejärjestelmän haltuunotolla.

7. Fyysiset hyökkäykset

   (a) Laitteen muuttaminen on mahdollista hyödyntämällä auki jätettyjä portteja, joita on muun muassa OBD ja CAN-väylässä sekä sisäisissä ja ulkoisissa verkoissa.

   (b) Laitetta voidaan vahingoittaa häiritsemällä sensoreita tai tunkeutumalla ajoneuvoon.

5.4 Riskianalyysi

Riskianalyysissä jokaiselle tunnistetulle riskille määritellään toteutumisen todennäköisyys ja vaikuttavuus, jonka perusteella riskille määritellään vakavuuden mukainen toimenpideehdotus.

Pääosassa rikollisesta toiminnasta on taloudellinen motiivi, ja lunnaiden vaatiminen on tehokas ja yksinkertainen tapa saada rahaa. Rikollisen kiristykseen käyttämän ajan on oltava suhteessa tuottoon, joten mitä helpommin ja useampaan kohteeseen voidaan hyökätä, sitä todennäköisemmin se tapahtuu. Chattopadhyay, Lam ja Tavva (2021) mukaan toteutuneista hyökkäyksistä yli 91 % on langattomia hyökkäyksiä, kuten pitkän kantaman etäpalvelinhyökkäyksiä (21 %) tai mobiilisovellushyökkäyksiä (8 %), ja loput fyysisiä, kuten CAN-väylän tietojen manipulointi (5 %). Muut motiivit, kuten seuranta- tai vahingoittamistarkoitus, on yksinkertaisuuden vuoksi jätetty tutkielmassa arvioinnista pois.

Maksamisen todennäköisyyteen puolestaan vaikuttaa toiminnan vaikuttavuus. Jos ajoneuvon fyysisiin toimintoihin, kuten ohjaukseen tai jarrutukseen, vaikutetaan samalla kun ovet lukitaan, on taipuminen kiristykseen todennäköisempää kuin vaikkapa tietojen sieppauksessa ja uhattaessa paljastaa esimerkiksi soitetut puhelut tai vieraillut osoitteet. Myöskään vaikutuk-

sen arvioinnissa ei ole huomioitu muita kuin rahallista motiivia, vaikka joissakin tapauksissa uhrin säännöllinen liikkumistieto tai ajoneuvossa tapahtuneet äänitetyt keskustelut voivat olla joillekin, esimerkiksi valtiollisille hyökkääjille, erittäin arvokkaita. Vaikuttavuus riippuu myös hyökkäyksen kohteesta, esimerkiksi navigointitietojen häirintä on logistiikkayhtiölle haitallisempaa ja rahallisesti arvokkaampaa kuin yksityishenkilölle. Tutkielman riskianalyysi on tehty pelkästään yksityishenkilön näkökulmasta.

Autonomisille autoille on kehitetty useita turvallisuusstandardeja, kuten ISOn (International Organization for Standardization) *Road vehicles — Functional safety, Road vehicles — Safety of the intended functionality* ja SAEn (Society of Automotive Engineers) *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems,* joissa on määritelty myös kyberturvallisuuden uhkakuvia ja luokittelutasoja. Tutkielmassa todennäköisyyttä ja vaikuttavuutta arvioidaan kuitenkin yksinkertaisemmin Digitaalisen turvallisuuden kehittäjäverkosto VAHTI (2022) suosittelemalla asteikolla 0–3 ja seurausten vakavuutta asteikolla 1–3. Asteikoissa 0 tarkoittaa, että riski ei toteudu missään olosuhteissa, 1 tarkoittaa, että riskin todennäköisyys on alhainen tai vaikutukset vähäiset, ja 3 tarkoittaa, että riskin todennäköisyys on korkea tai vaikutukset erittäin vakavia.

Kuvion 5 taulukkoon on riskikartoituksen jokaiseen kohtaan määritelty esimerkkitapaus, ja arvioitu todennäköisyys ja vaikuttavuus sekä niiden tulona riskiluku. Todennäköisyyden arviointi perustuu hyökkäyksen tekijän tuotto-panos suhteeseen, eli hyökkäyksellä saatavaan vaikuttavuuteen ja hyökkäyksen helppouteen. Tällöin hyökkäyksen todennäköisyys on korkeampi, jos

- se on tehtävissä etänä, ja
- sillä päästään vaikuttamaan ajoneuvon ohjainlaitteiden toimintaan, tai
- sen avulla voidaan varastaa henkilökohtaisesti arvokasta tietoa, kuten käyttäjätunnuksia ja salasanoja muihin palveluihin.

Esimerkkinä vaikka käyttäjän olinpaikka tai ajoreitit saadaan selville etähallintaohjelmiston tai tietoviihdejärjestelmän kautta etänä, tieto ei vaikuta ohjainlaitteisiin eikä ole suurimmalle osalle yksityiskäyttäjistä erityisen arvokasta tietoa (tapaus 1d, todennäköisyys 1). Sen sijaan aiheuttamalla järjestelmävika ajoneuvon eri osissa vaikutetaan ajoneuvon käyttöön ja

saadaan käyttäjän välitön huomio (tapaus 3c, todennäköisyys 3).

Vaikuttavuuden arviointi perustuu yksityishenkilön näkökulmaan. Vaikuttavuus on merkittävämpi, jos

- sillä saadaan ajoneuvo vikatilaan, tai
- sen käyttäytymistä muutetaan.

Esimerkiksi vaikka hyökkääjä saisi kaapattua etähallintaohjelmiston ja lukittua ovet, käyttäjä voi silti paikallisesti vaikuttaa asiaan omilla avaimillaan (tapaus 5a, vaikuttavuus 1). Fyysisellä hyökkäyksellä OBD-portin tai CAN-väylän kautta vastaavasti voidaan muuttaa ajoneuvon käyttäytymistä ja aiheuttaa turvallisuusuhka (tapaus 7a, vaikuttavuus 3).

Riski-luokka	Riskin tai sen uhkan kuvaus	Todennäköi-syys (0-3)	Vaikutta-vuus (1-3)	Riskiluku
1	**Ikävä toiminta / väärinkäytökset**			
1a	Viihdejärjestelmän kautta kerätään ajoneuvossa käydyt keskustelut ja paikannustiedot	1	1	**1**
1b	Ajoneuvon tiedonkäsittelyjärjestelmä ylikuormitetaan, ja aiheutetaan pysähtyminen tai onnettomuus	2	2	**4**
1c	Sensoritiedon väärentämisellä aiheutetaan ajoneuvon virhetilanne, pysähtyminen tai onnettomuus	2	2	**4**
1d	Käyttäjän yksityisyys vaarannetaan paljastamalla olinpaikka tai ajoreitit	1	1	**1**
1e	Käyttäjän tallettamia tietoja viihde- ja navigaatiojärjestelmässä muutetaan tai salataan	1	1	**1**
2	**Salakuuntelu / Sieppaus / Kaappaus & Tiedon sieppaus**			
2a	CAN-väylässä toimivien ohjainlaitteiden toiminta muutetaan telematiikan kautta	2	3	**6**
2b	Ajoneuvon etähallintaohjelmiston kautta lukitaan ovet tai käynnistetään moottori	3	1	**3**
2c	Puhelu- ja viestitiedot siepataan tai muutetaan	1	1	**1**
2d	Ulkoisen viestinnän skannauksella paljastetaan laite-, protokolla-, portti- tai palvelutietoja	1	1	**1**
2e	Etähallintaohjelmiston kautta varastetaan tallennettuja tietoja, kuten käyttäjätunnuksia ja salasanoja palveluihin (kuten Google, Apple tai Spotify)	3	2	**6**
2d	Ajoneuvon toimintaan vaikutetaan CAN väylän viestien uudelleenlähetyksellä aiheuttaen virhetilanne	2	3	**6**
3	**Katkot**			
3a	Käyttäjän ulkoinen viestintä estetään	2	1	**2**
3b	Haittaohjelmiston aiheuttama laitevaurio tai onnettomuus	2	2	**4**
3c	Järjestelmävika ajoneuvon eri osissa, sensori-, väylä- tai viihdejärjestelmätasolla	3	3	**9**
3d	Tukipalvelujen menetys estämällä kommunikaatio	0	1	**0**
4	**vahingot / IT-omaisuuden menetys**			
4a	Tietoviihdejärjestelmän tietojen keräys	1	1	**1**
5	**Virheet / häiriöt**			**0**
5a	Heikkoa salasanaa tai PIN-koodia hyväksikäytetään etähallintaohjelmiston käyttöön	3	1	**3**
5b	Liikennetiedotuksia tai reititystä häiritään	0	1	**0**
6	**Katastrofit**			
6a	Kommunikaatiota tai tietoviihdejärjestelmää häiriten estetään tiedotusten saanti	0	1	**0**
7	**Fyysiset hyökkäykset**			
7a	Ajoneuvon käyttäytymistä muutetaan käyttäen tunnettuja heikkouksia OBD-portissa tai CAN väylässä	1	3	**3**
7b	Ajoneuvoon tunkeudutaan käyttäen etähallintajärjestelmää tai langatonta avausjärjestelmää	2	2	**4**

Kuvio 5. Riskianalyysi.

Tapausten yhdistämisellä voidaan saavuttaa erilaisia lopputuloksia. Esimerkiksi käyttäjän manipuloinnilla, tai huonoimmillaan neljänumeroisen pin-koodin sekunneissa tapahtuvalla kokeilulla, saadaan yhteys etähallinto-ohjelmistoon, jota hyödyntäen saadaan selville ajoneuvon sijainti ja avataan ovet OBD-porttilaitteen tai haittaohjelmiston asentamiseksi.

Riskiluvun perusteella todennäköisimpiä ja käyttäjään eniten vaikuttavia hyökkäyksiä ovat toimet, joilla voidaan vaikuttaa ajoneuvon hallintaan (2a, 2d, 3c) tai varastaa henkilökohtaisia käyttäjätietoja (2e). Molemmat onnistuvat Pham ja Xiong (2021) ja Khatri, Shrestha ja Nam (2021) tutkimusten perusteella myös etäyhteydellä .

5.5 Auton osittainen analyysi

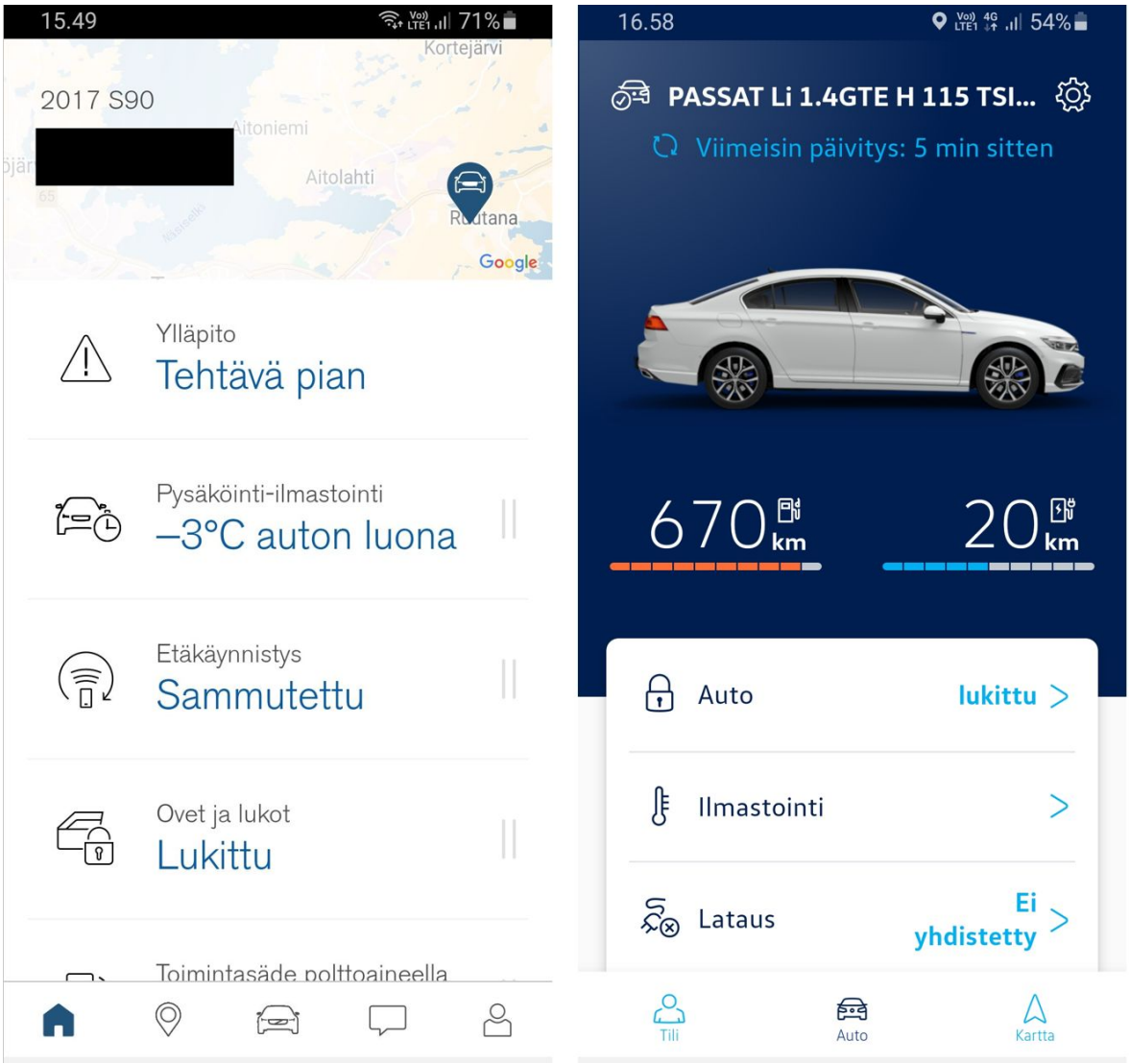
Tutkielmassa haluttiin selvittää vähintään tason 2 autonomialla varustetun nykyaikaisen, mutta jo useamman vuoden markkinoilla olleen auton mahdollisia heikkouksia. Auto olisi siis mahdollisesti ensimmäistä sukupolvea johon olisi tuotu autonomian ja reunalaskennan piirteitä. Auton ollessa pitkäikäinen hyödyke, auton suojauksen pitää kestää nykyiset ja tulevaisuuden kehittyneemmät hyökkäystekniikat. Vertailtavuuden vuoksi haluttiin tutkia useamman kuin yhden valmistajan ajoneuvo ja siihen liittyvät ratkaisut.

Tutkielmassa oli ensimmäisenä autona käytettävissä vuoden 2017 Volvo S90, jonka ominaisuuksiin kuuluu muun muassa mobiililaitteilla toimiva etähallintaohjelmisto, viihdejärjestelmä johon voi ladata omilla tunnuksilla toimivia sovelluksia, auton matkustajille jakama langaton verkko, ja tason 2 autonomia. Auto kykenee siis ajamaan itsenäisesti pitkiäkin matkoja, kun kuljettaja on valmiina puuttumaan toimintoihin, mikä varmistetaan säännöllisellä kosketuksella ohjauspyörään.

Toisena autona käytettiin vuoden 2020 Volkswagen Passat GTEtä, jonka ominaisuusluettelo on käytännössä sama kuin Volvon. Erottavana tekijänä oli valmistajan lisäksi jaetun langattoman verkon yhteystekniikka, Volvon vaatiessa erillisen SIM-kortin asentamisen tukeutui hieman uudempi Volkswagen sisäiseen eSIM ratkaisuun (palveluntarjoajana Cubic Telecom Limited). Kiinteä eSIM ratkaisu tietysti sitoo käyttäjän enemmän Volkswagenin omaan tarjontaan ja hinnoitteluun.

Riskianalyysin perusteella monet ulkoiset yhteysmahdollisuudet, omien tunnusten ja sovellusten käyttömahdollisuus, ja tason 2 autonomia tekevät ajoneuvoista monipuolisia kohteita. Samalla ne edustavat jo nyt hieman vanhempaa kehityssukupolvea, ja ovat siten mahdollisesti alttiimpia tulevaisuuden kehittyneempiin hyökkäyksiin. Ajoneuvojen fyysiset ominaisuudet kuten OBD- ja USB-portit ja CAN-väylät päätettiin jättää tutkielmassa huomioitta, koska tutkimusten mukaan jo yli 90 % hyökkäyksistä tapahtuu etänä tai langattomasti. Volvon etähallintaohjelmisto kuului käytännössä kaikkien myytävien ajoneuvojen varustukseen ensimmäisinä vuosina, ja Volkwagenistakin se löytyi lisävarusteena. Yleisyys ja mahdollisuus ladata sovellus verkkokaupasta vaikutti niiden valinnaksi ensisijaiseksi kohteeksi. Autojen mahdollisuus tarjota langaton verkko matkustajille, ja langattoman verkon ominaisuuden perusteella käytännössä myös lähellä oleville, vaikutti mielenkiintoiselta perinteiseltä tietoturvahaasteelta esimerkiksi mahdollisine avoimine portteineen. Tutkimuksen kirjallisuushaulla ei myöskään löytynyt näihin liittyvää tutkimustietoa.

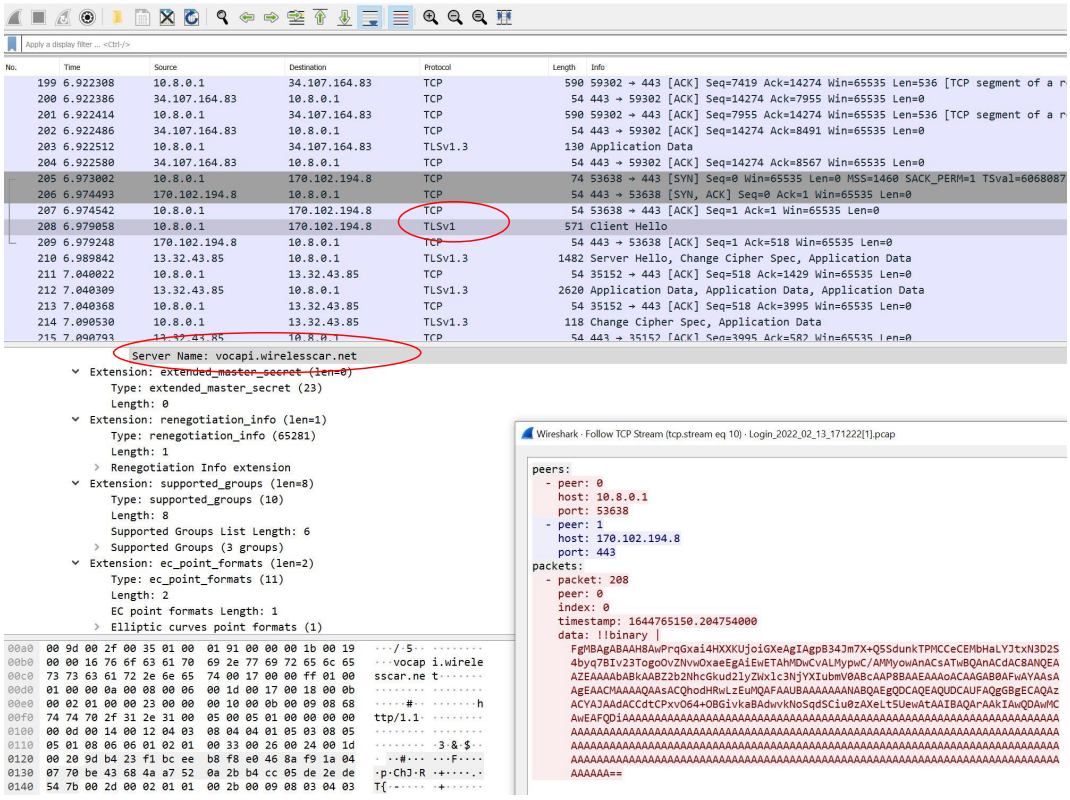
Autojen etähallintaohjelmistojen päänäkymät ovat kuviossa 6. Muun muassa autojen sijainnit, ovien lukitus, moottorin käynnistys ja pysäköinti-ilmastointi ovat nähtävillä ja hallittavissa suoraan päänäkymästä.



Kuvio 6. Ajoneuvojen etähallintaohjelmistojen päänäkymät.

5.5.1 Puhelimen etähallintaohjelmisto

Riskeihin 1d, 2b, 2c, 2e ja 2d liittyen etähallintasovellusten liikenne kaapattiin välimieshyökkäyksellä. Siihen käytettiin Android puhelinten sovelluskaupasta saatavaa *tPacketCapture* (Taosoftware Co., Ltd 2015) ohjelmistoa, joka hyödyntää Androidin virtuaalisen erillisverkon (Virtual Private Network, VPN) palvelua liikenteen tallentamiseen. Kaapattu liikenne puolestaan analysoitiin verkkoliikenteen asiantuntijoiden kehittämällä avoimen koodin *Wireshark* (Wireshark.org 2022) ohjelmistolla. Wiresharkin käyttöliittymästä on esimerkki kuviossa 7, jossa on valittuna asiakkaan aloittama TLSv1 tason kättely.



Kuvio 7. Wiresharkin verkkoliikenteen analyysinäkymä.

Etähallintaohjelmistojen kaikkia toimintoja ei käyty lävitse, vaan analyysiin otettiin vain sovellusten käynnistys ohjelmiston liikenteen ja arkkitehtuurin selvittämiseksi. Analysoidut liikennepaketit kutsuttuine palveluineen ja verkko-osoitteineen ovat saatavilla jaettuna kokonaisuudessa verkko-osoitteissa (Pasanen 2022c) ja (Pasanen 2022f).

Suurin osa Volvon etähallintaohjelmiston liikenteestä on TLS 1.2 ja TLS 1.3 salattua, mut-

ta joukossa on myös yksi (1) sovelluksen aloittama TLS 1 tason viestintä, joka on todettu haavoittuvaksi ja suositeltu korvattavaksi 1.2 tai korkeammilla versioilla. Palvelin kuitenkin vastaa asiakkaan pyyntöön TLS 1.3 tason vastauksella ja liikenne jatkuu hyvin suojattuna. Todennus- ja valtuutushyökkäyksen suorittaminen vaikuttaa näistä syistä hankalalta. Kaikki liikenne on salattua, eikä tunnuksia tai salasanoja välitetä tekstimuodossa. Oletettavasti helppokäyttöisyyden vuoksi käyttäjän todennukseen käytetään yksinkertaista tunnus-salasanaparia, eikä esimerkiksi kaksivaiheista tunnistusta.

Samat huomiot pätevät pitkälti myös Volkswagenin weConnect ohjelmistoon. weConnect tekee kuitenkin kolme (3) TLS 1 tason kutsua useampaan palveluun. Palvelimet vastaavat asiakkaan pyyntöihin TLS 1.2 ja TLS 1.3 tason vastauksilla ja liikenne jatkuu hyvin suojattuna. Sovelluksen käynnistyksessä oli myös merkittäviä eroja kutsujen määrässä ja kestossa, weConnectin tehdessä noin kaksi (2) kertaa enemmän kutsuja sovelluksen käynnistyksen kestäessä kuusi (6) kertaa pidempään (22 vs. 135 sekunttia).

Vaikka suurin osa käytetyistä palveluista on verkko-osoitteiden perusteella valmistajien omia palveluja Amazonin (AWS) pilvipalvelimilla, niin liikenteestä selviää, että käytössä on myös palveluja joita käytetään muihin tarkoituksiin, kuten valmistajan tuotteen kehittämiseen. Näitä ovat muun muassa Googlen *google-analytics.com*, Leanplumin *api.leanplum.com*, Microsoftin *in.appcenter.ms* ja Branch.ion *cdn.branch.io*. Sovelluksen toimintaan liittyviä palveluja, kuten sää, viestipalvelut tai kartat, sekä muita, joiden käyttötarkoitus on epäselvempi, haetaan muun muassa Facebookilta (*mqtt-mini.facebook.com, graph.facebook.com, b-graph.facebook.com, api.facebook.com, b-api.facebook.com*), Googlelta (*mtalk.google.com, maps.googleapis.com, firebaselogging-pa.googleapis.com, csi.gstatic.com, clients4.google.com*), Microsoftilta (*self.events.data.microsoft.com, skyapi.live.net, api.onedrive.com, config.edge.skype.com*), Samsungilta (*api. samsung.cloud*), Cubic Telecomilta (*autohmi-base.cubictelecom.com*) ja HEREltä (*weather.cc.api.here.com*).

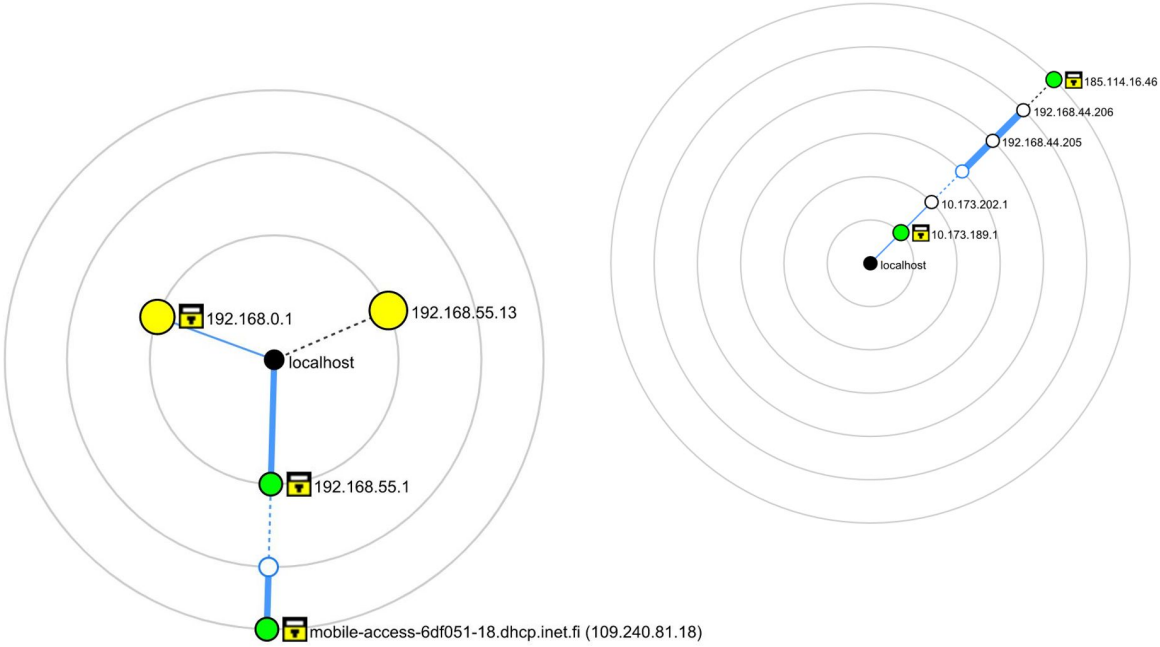
5.5.2 Auton jakama verkkoyhteys

Ajoneuvot kykenevät jakamaan erillisen langattoman verkon auton matkustajille. Sitä tutkittiin erityisesti riskeihin 2c, 2d, 3a, 4a ja 5a liittyen. Auton jakama langaton verkko on

erillinen ajoneuvon etähallinnan ja telemetrian käyttämästä, ja vaatii Volvossa erillisen SIM-kortin Volkswagenin käyttäessä eSIM-ratkaisua. Jaettua verkkoa vastaan päätettiin suorittaa verkon tutkiminen avoinna olevien porttien ja protokollien tunnistamiseksi. Autojen luomien vapaasti näkyvien WPA2 (Wi-Fi Protected Access) suojattujen verkkojen oletussalasanoja ei yritetty murtaa. Käyttäjät voivat molemmissa autoissa muuttaa sekä verkon nimeä että salasanaa. Volvossa verkon nimen on oltava 6–32 merkkinen, ja salasanan 10–63 merkkinen. Oletussalasana oli 11 merkkinen sisältäen isoja ja pieniä kirjaimia sekä numeroita, ei erikoismerkkejä. Volkswagenissa oletussalasana oli 12 merkkinen sisältäen isoja ja pieniä kirjaimia sekä numeroita ilman erikoismerkkejä. Tutkijat ovat havainneet WPA2 suojauksessa heikkouksia, mutta niiden hyödyntäminen vaatii fyysistä läheisyyttä kohteena olevaan verkkoon. Verkon kantaman sisällä oleva hyökkääjä voi esimerkiksi hyödyntämällä KRACKia (Key Reinstallation AttaCK) hyökätä yhteyden muodostukseen, ottaa käyttöön uuden salausavaimen, ja siepata ja purkaa tietoliikenteen omistamatta suojatun langattoman verkon tunnistetietoja (verkon salasanan vaihtaminen ei siis auta). (Bartoli, Medvet ja Onesti (2018), Euroopan unionin verkko- ja tietoturvavirasto (2017a) ja Akram, Saeed ja Daud (2018).)

Kuviossa 8 esitellään autojen verkkoympäristöt. Volvolla 192.168.55.1 on ajoneuvon yhdyskäytävä, 192.168.55.13 on analyysissa käytetty yhdistetty laite (kannettava tietokone), 109.240.81.18 on ajoneuvon ulkoinen osoite ja 192.168.0.1 on kaapelimodeemin tarjoama langaton yhdyskäytävä. Myös nämä ajoneuvoon liittymättömät osoitteet tutkittiin vertailun vuoksi. Volkswagenin verkkoyhteydet olivat ilmeisesti eSIM ratkaisun takia useamman verkkohypyn takana, yhdyskäytävä on osoitteessa 10.173.189.1 ja ajoneuvon ulkoinen osoite on 185.114.16.46.

Ajoneuvojen jakamaa verkkoa tutkittiin nmap.org (2022) avoimen ohjelmiston verkkoskannerin versiolla 7.92, kutsulla *"nmap -T4 -A -v <verkko-osoite>"*. NMap on verkonvalvojien vakiintunut työkalu, ja tutkielman keskittyessä lähinnä avointen porttien arvioimiseen ei nähty tarpeelliseksi käyttää useampia porttiskanneria. Käyttöliittymä ja osittainen Volvon tuloslistaus on esillä kuviossa 9, analyysit kokonaisuudessaan ovat saatavilla verkko-osoitteista (Pasanen 2022d) ja (Pasanen 2022a).

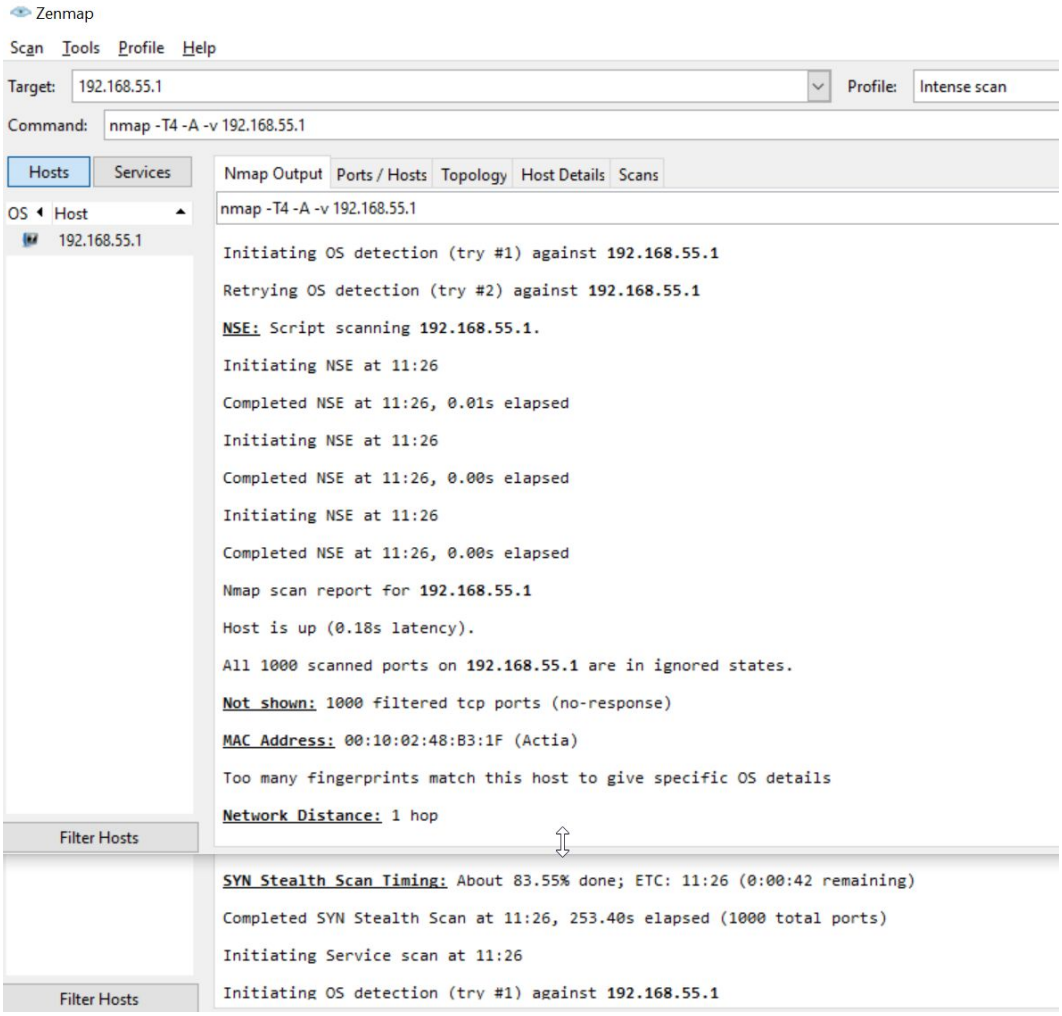


Kuvio 8. Ajoneuvojen verkkoympäristöt.

Volvon tulokset näyttivät selkeiltä ja osoittavat kaikkien porttien olevan kiinni. Edes käyttöjärjestelmä ei paljastunut. Ainoastaan MAC osoitteen takaa ilmeni todennäköinen yhdyskäytävän tekijä eli autoteollisuuden toimittaja Actia. Volkswagenin tulokset olivat vielä parempia, koska skannauksessa ei paljastunut edes yhdyskäytävän toimittajaa.

Volvon jaetun verkon ulkoinen nopeus ja osoite tarkistettiin Speedtest.net osoitteesta, ja löydetty ulkoinen osoite (mobile-access-6df051-18.dhcp.inet.fi, 109.240.81.18) skannattiin NMapin komennolla *"nmap -T4 -A -v -Pn 109.240.81.18"*. Komennolla suoritettiin syvempi analyysi ja parametrilla *"-Pn"* ohitettiin vastaamattomuus ping-kutsuun. Sama toiminta toistettiin Volkswagenille. Tulokset ovat saatavilla osoitteissa (Pasanen 2022e) ja (Pasanen 2022b). Kuviossa 10 on näkyvillä Volvolle suoritetun skannauksen tietoja ja muutaman portin suljettu tila. Kummankaann ulkoinen skannaus ei paljastanut haavoittuvuuksia kuten avoinna olevia portteja.

Vertailun vuoksi tehdyissä kannettavan tietokoneen ja kaapelimodeemin analyyseissä paljastui paljon enemmän hyökkääjälle hyödyllistä tietoa. Muun muassa laitteiden valmistajat, käyttöjärjestelmät, avoinna olevat portit, palvelut ja mahdollisuudet palvelunestohyökkäykseen olivat selkeästi esillä. Myös mahdollisuudet sekä verkkosivustojen välisten komentojen

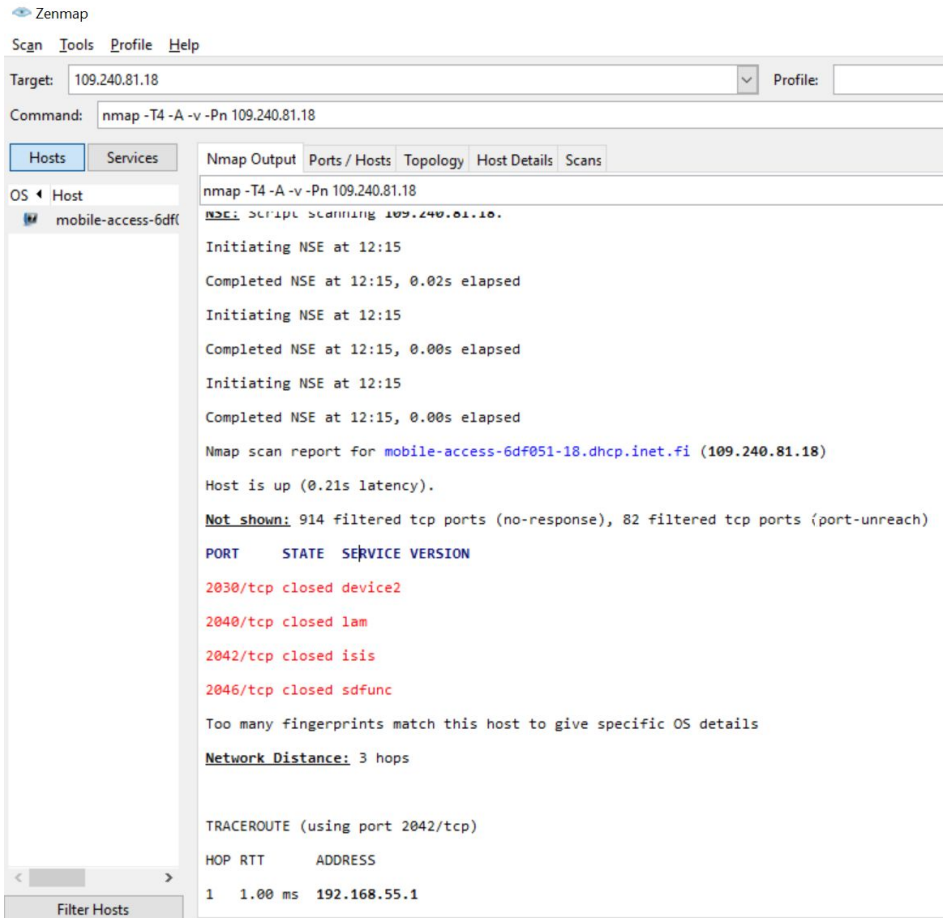


Kuvio 9. NMapin turvallisuusskannaus ajoneuvon tarjoamalle langattomalle verkolle.

(Cross-Site Scripting, XSS) ja verkkosivustojen välisten pyyntöjen (Cross-Site Request Forgery, CSRF) väärennökseen tulivat ilmi. Näitä analyysejä ei ole jaettu niiden paljastaessa liikaa tietoa käytetystä yksityisestä verkosta.

5.6 Analyysin tulokset

Ajoneuvojen tarjoamat langattomat verkot ja liitännät matkapuhelinverkkoon eivät paljastaneet käytetyillä analyysimenetelmillä suuria heikkouksia. Ainoastaan Volvon yhdyskäytävän valmistajan paljastuminen avaa seuraavia tutkintalinjoja mahdollisten ohjelmistovirheiden (nollapäivähaavoittuvuuksien) muodossa. Kohteena jaettu yhteys on kuitenkin houkutteleva,



Kuvio 10. NMapin turvallisuusskannaus Volvon ulkoiselle osoitteelle.

koska ohjelmistojen päivitysmahdollisuus avaa mahdollisuuden haittaohjelmistojen asentamiseen, ja mahdollisesti pääsyn autojen muihin järjestelmiin. Etähallintaohjelmistojen kohdalla löydettiin mahdollisuus välimieshyökkäykseen asiakkaiden aloittamien TLS 1 tason protokollan kohdalla. Huomautettakoon että analyysissä ei tarkistettu varmentavatko sovellukset kaikki käytetyt sertifikaatit. Tarkistamisen vaillinainen suorittaminen antaa Kuzlu, Fair ja Guler (2021) mukaan mahdollisuuden välimieshyökkäykseen, ja sitä käyttäen esimerkiksi käyttäjän tunnistetietojen varastamiseen. Tutkimuksessa ei myöskään lähdetty kokeilemaan viestien toiston antamia mahdollisuuksia saada tarvittavia käyttöoikeuksia. Mahdollisesti helppokäyttöisyyden vuoksi etähallintasovelluksissa ei ole käyttäjätunnus-salasanaparia vahvempaa tunnistautumista. Yksinkertainen tunnistus antaa hyökkääjälle mahdollisuuden hyödyntää esimerkiksi käyttäjän manipulaatiota tunnistetietojen saamiseksi. Koska sovellukset ovat vapaasti ladattavissa pääsy ajoneuvon tietoihin ja hallintaan on tämän jälkeen yksin-

kertaista. Etähallintaohjelmistoihin olisikin syytä tehdä halukkaille käyttäjille mahdollisuus määritellä vahvempi tunnistautuminen, esimerkiksi kaksivaiheisella tunnistuksella.

Etähallintasovelluksien liikenteestä paljastui suuri määrä liikennettä kolmansien osapuolten palvelimille. Niihin liittyvää sisältöä ei tutkittu tarkemmin, mutta Volvo Cars (2022) ja Volkswagen AG (2022) ilmoittavat, että kerättäviä henkilökohtaisia GDPRn alaisia tietoja voidaan välittää kolmansille osapuolille, euroopan ulkopuolelle ja ei välttämättä anonymisoidussa tai pseudonomisoidussa muodossa. Käyttäjätietojen keräämisen lisäksi Volkswagen mainitsee markkinointitarkoituksiin osoitekirjasta kerättävät ensisijaiset yhteistyökumppanit, kalenterista poimittavat toteutuneet tapaamiset sekä GPSn avulla kerättävät sijaintitiedot. Lisäksi Volkswagenin mukaan tietoja voidaan rikastaa esimerkiksi osoitteen perusteella täydennettävillä sosioekonomisilla ja sosiodemografisilla tiedoilla.

Auton telematiikka, sovellusten ja käyttöjärjestelmien asennusmahdollisuus, USB ja Bluetooth liitännät, OBD-portti, sensorit ja CANBUS-väylä jätettiin työmäärän ja käytettävissä olevien työkalujen takia tutkimuksen ulkopuolelle. Lisäksi Khatri, Shrestha ja Nam (2021) mukaan pääsy CANBUS-väylään tarjoaa käytännössä rajattomat hallintamahdollisuudet, eikä lisäarvoa suoritettavasta tutkimisesta olisikaan välttämättä saatu.

5.7 Pohdinta

Suoritetun tutkimuksen perusteella jaettuun yhteyteen liittyvät ilmiselvät riskit, esimerkiksi avointen porttien kautta, ovat valmistajien toimesta pyritty sulkemaan. Ainoastaan yhdyskäytävän valmistajan paljastuminen avaa selkeämpää tutkimuslinjaa haavoittuvuuksille. Toisaalta tutkimuksessa ei pyrittykään tarkistamaan esimerkiksi kuinka hyvin autojen sovellusten lataaminen, asentaminen ja suorittaminen on eristetty auton muista ohjelmistoista. Muissa tutkimuksissa on asennettavien sovellusten kautta löydetty useita keinoja haittaohjelmistojen asentamiseen ja pääsyyn ajoneuvon sovelluksiin ja väylätoimintoihin. Normaaliin sovelluskehitykseen liittyvä säännöllinen tietoturvatestaus ja ohjelmistojen päivittäminen haavoittuvuuksia vastaan pitäisi kuulua jo nyt myös autovalmistajien ja alihankkijoiden toimenpidelistalle.

Etähallintasovelluksen kohdalla toimenpide-ehdotuksia on helppo nimetä. Käyttäjän kohdal-

la sellaisia ovat huolehtiminen riittävän turvallisesta salasanasta sekä varautumisesta mahdolliseen käyttäjän manipulointiin (tunnuksia ei ole syytä jakaa). Näistä on syytä huolehtia heti ohjelmiston käyttöönotossa. Valmistajien puolestaan pitäisi tarjota käyttäjille mahdollisuus suojata sovelluksen toiminnot vahvemmalla tunnistuksella, esimerkiksi kaksivaiheisesti, mahdollisimman nopeasti.

Vetoamalla oikeutettuun etuun (GDPR 6 artiklan kohta 1 f, Euroopan Unioni (2016)) valmistajat ottavat laajat vapaudet kerätä yksityisiä käyttäjätietoja, ja mahdollisesti anonymisoimatta tai pseudonomisoimatta siirtää niitä kolmansille osapuolille myös euroopan ulkopuolelle. Käyttäjien yksityisyyden parantamiseksi näihin liittyviä suostumuskohtia pitäisikin pystyä yksilöimään tarkemmin.

Tutkimus kohdistui vain kahden valmistajan autoihin, eikä mahdollisia jatkotutkimuslinjoja viety eteenpäin. Näitä olisivat olleet muun muassa sertifikaattien varmistamiskäytännöt, kaapatun liikenteen toisto, yhdyskäytävän ohjelmiston haavoittuvaisuuksien tutkinta, käyttäjien yksityisyyteen liittyvät kysymykset ja sovellusten päivitys- ja asennusmahdollisuudet. Varsinkin ohjelmistojen asentamisen kautta tapahtuneita hyökkäysmahdollisuuksia löytyy tutkimuksista paljon, ja onnistuessaan ne ovat johtaneet mahdollisuuteen saada ajoneuvo täydellisesti hallintaan. Reunalaskennan perustutkimuksen puolella sivukanavien käyttö sekä hyökkäyksiin että erityisesti hyödyntäminen puolustuksen tehostamiseen vaikutti mielenkiintoiselta jatkotutkimusaiheelta. Yksityisyyden suojan tutkiminen muun muassa välitettävien tietojen, käsittelevien osapuolien, tietojen tarpeellisuuden sekä tietojen käytön osalta avaisi kokonaisen uuden jatkotutkimusalueen. Tutkimusta olisi myös hyvä täydentää riskikartoituksen osalta käyttämällä useampaa arvioijaa, arvioida myös muita kuin yksityishenkilön näkökulma, sekä suorittaa verkon tutkimus useammalla skannerilla. Skannereita ja muita täydentäviä työkaluja, kuten salasanojen murtajia ja langattoman verkon penetraatiotyökaluja löytyy muun muassa ilmaisesta Kali-Linux paketista (kali.org (2022)).

6 Yhteenveto

Tutkielman tavoitteena oli löytää ja koota yhteen reunalaskennan tietoturvaan kohdistuvia haasteita ja käsitellä ongelmakohtiin kehitettyjä ratkaisuja. Reunatoimijoista tarkasteltiin modernia autoa ja pyrittiin löytämään mahdollisia avoimia tutkimusalueita, ratkaisumalleja ja suosituksia, joilla erityisesti autojen reunalaskennan tietoturvaa voidaan parantaa. Itseohjautuvien ajoneuvojen ajotestien alkamisesta lähtien autoihin kohdistuneiden kyberhyökkäysten määrä on 6-kertaistunut vuodesta 2010 vuoteen 2018, ja yli 9 hyökkäystä kymmenestä on jo ollut langattomia.

Tutkielmassa selvitettiin nykyaikaisen, mutta jo useamman vuoden markkinoilla olleen auton mahdollisia heikkouksia. Riskianalyysin perusteella monet ulkoiset yhteysmahdollisuudet, omien tunnusten ja sovellusten käyttömahdollisuus sekä tason 2 autonomia tekevät ajoneuvoista monipuolisia kohteita. Ajoneuvojen fyysiset ominaisuudet kuten OBD- ja USB-portit ja CAN-väylät päätettiin jättää tutkielmassa huomioitta, koska tutkimusten mukaan jo yli 90 % hyökkäyksistä tapahtuu etänä tai langattomasti. Autojen etähallintaohjelmistot sekä mahdollisuus tarjota langaton verkko matkustajille vaikuttivat mielenkiintoisilta kohteilta, eikä tutkimuksen kirjallisuudesta löytynyt näihin liittyvää tutkimustietoa.

Suoritettujen analyysien perusteella valmistajat olivat huomioineet ilmiselvät riskit, kuten turhat avoimet portit ja selväkielisen liikenteen. Liikenteestä kuitenkin paljastui haavoittuvaksi tiedettyä kutsuja, ja yhdyskäytävän valmistajan paljastuminen avasi myös mahdollisen hyökkäyslinjan. Etähallintasovelluksista oli ilmeisesti pyritty tekemään helppokäyttöisiä, ja sen perusteella pitäydytty yksinkertaisessa tunnus-salasana yhdistelmässä. Tällöin kuka tahansa ohjelmiston ladannut tunnukset tietäessään pääsee käsiksi ajoneuvon ohjaukseen ja käyttäjien yksityisiin tietoihin. Mahdollisuudella parempaan tunnistautumiseen, esimerkiksi kaksivaiheisella tunnistuksella, väärinkäytön mahdollisuutta voitaisiin pienentää. Liikenteestä paljastui myös paljon viestintää kolmansien osapuolten kanssa. Vetoamalla oikeutettuun etuun valmistajat ottavat laajat vapaudet kerätä yksityisiä käyttäjätietoja, ja mahdollisesti anonymisoimatta tai pseudonomisoimatta siirtää niitä kolmansille osapuolille myös euroopan ulkopuolelle. Käyttäjien yksityisyyden parantamiseksi näihin liittyviä suostumuskohtia pitäisikin pystyä yksilöimään tarkemmin.

Autonomisten ajoneuvojen markkinoiden jatkaessa nopeaa kasvuaan, reunalaskennan tarve, integroituminen muihin järjestelmiin ja tietoturvahaasteet tulevat kasvamaan. Rajanvedot valmistajien ja käyttäjien vastuiden, sekä käyttäjien yksityisyyden ja valmistajien oikeuksien välillä, yhdessä viranomaismääräyksien kehittymisen ja valmistajien halun toimittaa nopeasti ratkaisuja kiihtyvään kysyntään on jatkossakin haastava pelikenttä. Tutkimusalueena reunalaskenta ja autonomisten ajoneuvojen rajapinta tuleekin olemaan erittäin kiinnostava.

Lähteet

Achakey. 2022. *Share your car key with ACHAKEY.* Saatavilla WWW-muodossa, https://achakey.net/, viitattu 29.1.2022.

Akram, Zeeshan, Muhammad Anwaar Saeed ja Marriam Daud. 2018. "Real time exploitation of security mechanisms of residential WLAN access points". Teoksessa *2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET),* 1–5. https://doi.org/10.1109/ICOMET.2018.8346378.

Aliyu, F., T. Sheltami, A. Mahmoud, L. Al-Awami ja A Yasar. 2021. "Detecting man-in-the-middle attack in fog computing for social media". *Computers, Materials, and Continua* 69:1159–1181. https://doi.org/10.32604/cmc.2021.016938.

Aliyu, Farouq, Tarek Sheltami ja Elhadi M. Shakshuki. 2018. "A Detection and Prevention Technique for Man in the Middle Attack in Fog Computing". *Procedia Computer Science* 141:24–31. ISSN: 1877-0509. https://doi.org/10.1016/j.procs.2018.10.125.

Aloul, Fadi, Syed Zahidi ja Wassim El-Hajj. 2009. "Two factor authentication using mobile phones". Teoksessa *2009 IEEE/ACS International Conference on Computer Systems and Applications,* 641–644. https://doi.org/10.1109/AICCSA.2009.5069395.

Alwakeel, Ahmed M. 2021. "An Overview of Fog Computing and Edge Computing Security and Privacy Issues". *Sensors* 21 (24). ISSN: 1424-8220. https://doi.org/10.3390/s21248226.

Alwarafy, Abdulmalik, Khaled A. Al-Thelaya, Mohamed Abdallah, Jens Schneider ja Mounir Hamdi. 2021. "A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things". *IEEE Internet of Things Journal* 8 (6): 4004–4022. https://doi.org/10.1109/JIOT.2020.3015432.

Apple. 2021. *Security of runtime process in iOS and iPadOS.* Saatavilla WWW-muodossa, https://support.apple.com/fi-fi/guide/security/sec15bfe098e/web, viitattu 28.5.2022.

Baktir, Ahmet Cihat, Atay Ozgovde ja Cem Ersoy. 2017. “How Can Edge Computing Benefit From Software-Defined Networking: A Survey, Use Cases, and Future Directions”. *IEEE Communications Surveys Tutorials* 19 (4): 2359–2391. https://doi.org/10.1109/COMST.2017.2717482.

Bartoli, Alberto, Eric Medvet ja Filippo Onesti. 2018. “Evil twins and WPA2 Enterprise: A coming security disaster?” *Computers & Security* 74:1–11. ISSN: 0167-4048. https://doi.org/10.1016/j.cose.2017.12.011.

BBC News. 2021. *Lars Vilks: Muhammad cartoonist killed in traffic collision.* Saatavilla WWW-muodossa, https://www.bbc.com/news/world-europe-58783998, viitattu 22.1.2022.

Bhargavan, Karthikeyan, Bruno Blanchet ja Nadim Kobeissi. 2017. “Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate”. Teoksessa *2017 IEEE Symposium on Security and Privacy (SP),* 483–502. https://doi.org/10.1109/SP.2017.26.

BMW. 2020. *Full guide to BMW software updates.* Saatavilla WWW-muodossa, https://www.bmw.com/en/innovation/bmw-software-update.html, viitattu 29.1.2022.

Bonomi, Flavio, Rodolfo Milito, Jiang Zhu ja Sateesh Addepalli. 2012. “Fog Computing and Its Role in the Internet of Things”. Teoksessa *Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing,* 13–16. MCC ’12. New York, NY, USA: Association for Computing Machinery. ISBN: 9781450315197. https://doi.org/10.1145/2342509.2342513.

Chattopadhyay, Anupam, Kwok-Yan Lam ja Yaswanth Tavva. 2021. “Autonomous Vehicle: Security by Design”. *IEEE Transactions on Intelligent Transportation Systems* 22 (11): 7015–7029. https://doi.org/10.1109/TITS.2020.3000797.

Chen, Eric Y., Yutong Pei, Shuo Chen, Yuan Tian, Robert Kotcher ja Patrick Tague. 2014. “OAuth Demystified for Mobile Application Developers”. Teoksessa *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security,* 892–903. CCS ’14. Scottsdale, Arizona, USA: Association for Computing Machinery. ISBN: 9781450329576. https://doi.org/10.1145/2660267.2660323.

Chen, Qi Alfred, Zhiyun Qian ja Z. Morley Mao. 2014. “Peeking into Your App without Actually Seeing It: UI State Inference and Novel Android Attacks”. Teoksessa *23rd USENIX Security Symposium (USENIX Security 14),* 1037–1052. San Diego, CA: USENIX Association, elokuu. ISBN: 978-1-931971-15-7. https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/chen.

Chowdhury, Abdullahi, Gour Karmakar, Joarder Kamruzzaman, Alireza Jolfaei ja Rajkumar Das. 2020. “Attacks on Self-Driving Cars and Their Countermeasures: A Survey”. *IEEE Access* 8:207308–207342. https://doi.org/10.1109/ACCESS.2020.3037705.

Cirani, Simone, Marco Picone, Pietro Gonizzi, Luca Veltri ja Gianluigi Ferrari. 2015. “IoT-OAS: An OAuth-Based Authorization Service Architecture for Secure Services in IoT Scenarios”. *IEEE Sensors Journal* 15 (2): 1224–1234. https://doi.org/10.1109/JSEN.2014.2361406.

Cisco. 2020. *Cisco Annual Internet Report (2018–2023) White Paper.* Saatavilla WWW-muodossa, https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html, viitattu 9.3.2020.

Clark, Shane S., Benjamin Ransford, Amir Rahmati, Shane Guineau, Jacob Sorber, Wenyuan Xu ja Kevin Fu. 2013. “WattsUpDoc: Power Side Channels to Nonintrusively Discover Untargeted Malware on Embedded Medical Devices”. Teoksessa *2013 USENIX Workshop on Health Information Technologies (HealthTech 13).* Washington, D.C.: USENIX Association, elokuu. https://www.usenix.org/conference/healthtech13/workshop-program/presentation/clark.

Digitaalisen turvallisuuden kehittäjäverkosto VAHTI. 2022. *Digiturvallisuuden hallinta – tukimateriaali digiturvan kehittäjille.* Saatavilla WWW-muodossa, https://dvv.fi/documents/16079645/0/Digiturvallisuuden_hallinta_NETTI_3105_2021.pdf/f6243645-79e2-81f7-5c3d-ccf2e972b2ec/Digiturvallisuuden_hallinta_NETTI_3105_2021.pdf?t=1622534350192, viitattu 12.2.2022.

Euro NCAP, European New Car Assessment Programme. 2022. *Safety Campaigns.* Saatavilla www-muodossa, https://www.euroncap.com/en/vehicle-safety/safety-campaigns/2020-assisted-driving-tests/whats-new/, viitattu 12.2.2022.

Euroopan Unioni. 2016. *EU yleinen tietosuoja-asetus. Artikla 6. "Käsittelyn lainmukaisuus".* Saatavilla WWW-muodossa, https://gdprinfo.eu/fi/fi-article-6, viitattu 25.9.2022.

Euroopan unionin verkko- ja tietoturvavirasto. 2017a. *An overview of the Wi-Fi WPA2 vulnerability.* https://www.enisa.europa.eu/publications/info-notes/an-overview-of-the-wi-fi-wpa2-vulnerability.

———. 2017b. *Baseline security recommendations for IoT in the context of critical information infrastructures.* European Network / Information Security Agency. ISBN: 978-92-9204-236-3. https://doi.org/10.2824/03228.

Felt, Adrienne Porter, Erika Chin, Steve Hanna, Dawn Song ja David Wagner. 2011. "Android Permissions Demystified". Teoksessa *Proceedings of the 18th ACM Conference on Computer and Communications Security,* 627–638. CCS '11. Chicago, Illinois, USA: Association for Computing Machinery. ISBN: 9781450309486. https://doi.org/10.1145/2046707.2046779.

Fernandes, Earlence, Jaeyeon Jung ja Atul Prakash. 2016. "Security Analysis of Emerging Smart Home Applications". Teoksessa *2016 IEEE Symposium on Security and Privacy (SP),* 636–654. https://doi.org/10.1109/SP.2016.44.

Fernandes, Earlence, Justin Paupore, Amir Rahmati, Daniel Simionato, Mauro Conti ja Atul Prakash. 2016. "FlowFence: Practical Data Protection for Emerging IoT Application Frameworks". Teoksessa *25th USENIX Security Symposium (USENIX Security 16),* 531–548. Austin, TX: USENIX Association, elokuu. ISBN: 978-1-931971-32-4. https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/fernandes.

Fernandes, Earlence, Amir Rahmati, Jaeyeon Jung ja Atul Prakash. 2018. "Decentralized Action Integrity for Trigger-Action IoT Platforms". *Proceedings 2018 Network and Distributed System Security Symposium,* https://doi.org/10.14722/ndss.2018.23119.

Firouzi, Farshad, Bahar Farahani ja Alexander Marinšek. 2021. "The convergence and interplay of edge, fog, and cloud in the AI-driven Internet of Things (IoT)". *Information Systems,* 101840. ISSN: 0306-4379. https://doi.org/10.1016/j.is.2021.101840.

Frantti, Tapio, ja Markku Korkiakoski. 2022. “Security Controls for Smart Buildings with Shared Space”. Teoksessa *2022 6th International Conference on Smart Grid and Smart Cities (ICSGSC).* Accepted conference paper. http://www.csgsc.net/.

Google. 2022a. *Application Sandbox.* Saatavilla WWW-muodossa, https://source.android.com/security/app-sandbox, viitattu 28.5.2022.

———. 2022b. *Googlen suorittama datan anonymisointi.* Saatavilla WWW-muodossa, https://policies.google.com/technologies/anonymization?hl=fi, viitattu 8.1.2022.

Greenberg, Andy. 2017. *The Reaper IoT Botnet Has Already Infected a Million Networks.* Saatavilla WWW-muodossa, https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/, viitattu 8.1.2022.

Ho, Grant, Derek Leung, Pratyush Mishra, Ashkan Hosseini, Dawn Song ja David Wagner. 2016. “Smart Locks: Lessons for Securing Commodity Internet of Things Devices”. Teoksessa *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security,* 461–472. ASIA CCS ’16. Xi’an, China: Association for Computing Machinery. ISBN: 9781450342339. https://doi.org/10.1145/2897845.2897886.

Huawei. 2018. *Huawei’s Global Industry Vision 2025.* Saatavilla WWW-muodossa, https://www.huawei.com/minisite/giv/Files/whitepaper_en_2018.pdf, viitattu 2018.

Iltasanomat. 2021. *Uusi tutkimustulos julki: Tämä on nyt suomalaisille auton tärkein käyttötarkoitus – koronan vaikutus näkyy ja tuntuu.* Saatavilla WWW-muodossa, https://www.is.fi/autot/art-2000008251727.html, viitattu 29.1.2022.

International Organization for Standardization, ISO. 2018. *Road vehicles — Functional safety.* Saatavilla WWW-muodossa, https://www.iso.org/standard/68383.html, viitattu 12.2.2022.

———. 2019. *Road vehicles — Safety of the intended functionality.* Saatavilla WWW-muodossa, https://www.iso.org/standard/70939.html, viitattu 12.2.2022.

Iorga, Michaela, Larry Feldman, Robert Barton, Michael J Martin, Nedim S Goren, Charif Mahmoudi ym. 2018. “Fog computing conceptual model”, https://doi.org/10.6028/NIST.SP.500-325.

Istiaque Ahmed, Kazi, Mohammad Tahir, Mohamed Hadi Habaebi, Sian Lun Lau ja Abdul Ahad. 2021. “Machine Learning for Authentication and Authorization in IoT: Taxonomy, Challenges and Future Research Direction”. *Sensors* 21 (15). ISSN: 1424-8220. https://doi.org/10.3390/s21155122.

Jagielski, Matthew, Nicholas Jones, Chung-Wei Lin, Cristina Nita-Rotaru ja Shinichi Shiraishi. 2018. “Threat Detection for Collaborative Adaptive Cruise Control in Connected Cars”. Teoksessa *Proceedings of the 11th ACM Conference on Security and Privacy in Wireless and Mobile Networks,* 184–189. WiSec ’18. Stockholm, Sweden: Association for Computing Machinery. ISBN: 9781450357319. https://doi.org/10.1145/3212480.3212492.

Jan, Mian Ahmad, Fazlullah Khan, Muhammad Alam ja Muhammad Usman. 2019. “A payload-based mutual authentication scheme for Internet of Things”. *Future Generation Computer Systems* 92:1028–1039. ISSN: 0167-739X. https://doi.org/10.1016/j.future.2017.08.035.

Jin, Andrew Teoh Beng, David Ngo Chek Ling ja Alwyn Goh. 2004. “Biohashing: two factor authentication featuring fingerprint data and tokenised random number”. *Pattern Recognition* 37 (11): 2245–2255. ISSN: 0031-3203. https://doi.org/10.1016/j.patcog.2004.04.011.

kali.org. 2022. *Open-source Linux distribution geared towards various information security tasks.* Saatavilla www-muodossa, https://www.kali.org/, viitattu 12.2.2022.

Karapanos, Nikolaos, Claudio Marforio, Claudio Soriente ja Srdjan Capkun. 2015. “Sound-Proof: Usable Two-Factor Authentication Based on Ambient Sound”. Teoksessa *24th USENIX Security Symposium (USENIX Security 15),* 483–498. Washington, D.C.: USENIX Association, elokuu. ISBN: 978-1-939133-11-3. https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/karapanos.

Khatri, Narayan, Rakesh Shrestha ja Seung Yeob Nam. 2021. “Security Issues with In-Vehicle Networks, and Enhanced Countermeasures Based on Blockchain”. *Electronics* 10 (8). ISSN: 2079-9292. https://doi.org/10.3390/electronics10080893.

KIA. 2022. *Kia connect.* Saatavilla WWW-muodossa, https://owners.kia.com/us/en/about-uvo-link.html, viitattu 29.1.2022.

Krishna, Ritika Raj, Aanchal Priyadarshini, Amitkumar V. Jha, Bhargav Appasani, Avireni Srinivasulu ja Nicu Bizon. 2021. “State-of-the-Art Review on IoT Threats and Attacks: Taxonomy, Challenges and Solutions”. *Sustainability* 13 (16). ISSN: 2071-1050. https://doi.org/10.3390/su13169463.

Kuzlu, M., C. Fair ja O Guler. 2021. “Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity”. *Discov Internet Things* 1 (7). https://doi.org/10.1007/s43926-020-00001-4.

Li, Hong, Yunhua He, Limin Sun, Xiuzhen Cheng ja Jiguo Yu. 2016. “Side-channel information leakage of encrypted video stream in video surveillance systems”. Teoksessa *IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications,* 1–9. https://doi.org/10.1109/INFOCOM.2016.7524621.

Li, Mengyuan, Yan Meng, Junyi Liu, Haojin Zhu, Xiaohui Liang, Yao Liu ja Na Ruan. 2016. “When CSI Meets Public WiFi: Inferring Your Mobile Phone Password via WiFi Signals”. Teoksessa *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security,* 1068–1079. CCS ’16. Vienna, Austria: Association for Computing Machinery. ISBN: 9781450341394. https://doi.org/10.1145/2976749.2978397.

Lin, Jie, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang ja Wei Zhao. 2017. “A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications”. *IEEE Internet of Things Journal* 4 (5): 1125–1142. https://doi.org/10.1109/JIOT.2017.2683200.

Livadas, Carl, Robert Walsh, David Lapsley ja W. Timothy Strayer. 2006. “Usilng Machine Learning Technliques to Identify Botnet Traffic”. Teoksessa *Proceedings. 2006 31st IEEE Conference on Local Computer Networks,* 967–974. https://doi.org/10.1109/LCN.2006.322210.

Lu, Youshui, Yong Qi, Saiyu Qi, Fuyou Zhang, Wei Wei, Xu Yang, Jingning Zhang ja Xinpei Dong. 2021. “Secure Deduplication-based Storage Systems with Resistance to Side-Channel Attacks via Fog Computing”. *IEEE Sensors Journal,* 1–1. https://doi.org/10.1109/JSEN.2021.3052782.

Mahmood, Zaigham. 2018. *Fog Computing: Concepts, Frameworks and Technologies.* 291. Springer International Publishing. https://doi.org/10.1007/978-3-319-94890-4.

McIntosh, Michael, ja Paula Austel. 2005. "XML Signature Element Wrapping Attacks and Countermeasures". Teoksessa *Proceedings of the 2005 Workshop on Secure Web Services,* 20–27. SWS '05. Fairfax, VA, USA: Association for Computing Machinery. ISBN: 1595932348. https://doi.org/10.1145/1103022.1103026.

Mercedes Benz. 2022. *Mercedes me connect.* Saatavilla WWW-muodossa, https://www.mercedes-benz.fi/passengercars/being-an-owner/mercedes-me-connect/mercedes-me-connect.module.html, viitattu 29.1.2022.

Miller, Charlie, ja Chris Valasek. 2015. "Remote exploitation of an unaltered passenger vehicle". *Black Hat USA* 2015 (S 91). https://www.academia.edu/download/53311546/Remote_Car_Hacking.pdf.

Mosenia, Arsalan, ja Niraj K. Jha. 2017. "A Comprehensive Study of Security of Internet-of-Things". *IEEE Transactions on Emerging Topics in Computing* 5 (4): 586–602. https://doi.org/10.1109/TETC.2016.2606384.

Naha, Ranesh Kumar, Saurabh Garg, Dimitrios Georgakopoulos, Prem Prakash Jayaraman, Longxiang Gao, Yong Xiang ja Rajiv Ranjan. 2018. "Fog Computing: Survey of Trends, Architectures, Requirements, and Research Directions". *IEEE Access* 6:47980–48009. https://doi.org/10.1109/ACCESS.2018.2866491.

Ni, Jianbing, Xiaodong Lin ja Xuemin Sherman Shen. 2019. "Toward Edge-Assisted Internet of Things: From Security and Efficiency Perspectives". *IEEE Network* 33 (2): 50–57. https://doi.org/10.1109/MNET.2019.1800229.

nmap.org. 2022. *NMap Free Security Scanner.* Saatavilla www-muodossa, https://nmap.org/, viitattu 12.2.2022.

Ometov, Aleksandr, Oliver Liombe Molua, Mikhail Komarov ja Jari Nurmi. 2022. "A Survey of Security in Cloud, Edge, and Fog Computing". *Sensors* 22 (3). ISSN: 1424-8220. https://doi.org/10.3390/s22030927.

OpenEdge Computing. 2021. *OpenEDGEComputing.* Saatavilla WWW-muodossa, https://www.openedgecomputing.org/, viitattu 10.2021.

Otoum, Yazan, Dandan Liu ja Amiya Nayak. 2019. "DL-IDS: a deep learning–based intrusion detection framework for securing IoT". *Transactions on Emerging Telecommunications Technologies* 33 (3): e3803. https://doi.org/10.1002/ett.3803.

Paganini, Pierluigi. 2022. *Y2k22 bug in Microsoft Exchange causes failure in email delivery.* Saatavilla WWW-muodossa, https://securityaffairs.co/wordpress/126205/security/y2k22-bug-microsoft-exchange.html, viitattu 1.1.2022.

Parikh, Shalin, Dharmin Dave, Reema Patel ja Nishant Doshi. 2019. "Security and Privacy Issues in Cloud, Fog and Edge Computing". *Procedia Computer Science* 160:734–739. ISSN: 1877-0509. https://doi.org/10.1016/j.procs.2019.11.018.

Pasanen, Mauno. 2021. *Sumulaskennan hyödyntäminen esineiden internetissä.* Toimittanut Jyväskylän yliopisto. http://www.urn.fi/URN:NBN:fi:jyu-202112155968.

———. 2022a. *Volkswagenin tarjoaman langattoman verkon analyysi.* Saatavilla WWW-muodossa, https://drive.google.com/file/d/1IJ_8jxW_6kLjTTmX5Ryrxr19-DyF4jyC/view?usp=sharing, viitattu 30.4.2022.

———. 2022b. *Volkswagenin tarjoaman langattoman verkon ulkoisen osoitteen analyysi.* Saatavilla WWW-muodossa, https://drive.google.com/file/d/1cykQa4s7WkBRV4-lX3Xm1Oiay5Kad_mp/view?usp=sharing, viitattu 30.4.2022.

———. 2022c. *Volvon etähallintasovelluksen liikennekaappaus.* Saatavilla WWW-muodossa, https://drive.google.com/file/d/1yBq1wl_J2S1p9LuwKe_Xbv49kA-0kIPB/view?usp=sharing, viitattu 13.3.2022.

———. 2022d. *Volvon tarjoaman langattoman verkon analyysi.* Saatavilla WWW-muodossa, https://drive.google.com/file/d/1cXyv5pD5mzsXwk4jmqoSdH9GTOb-X8la/view?usp=sharing, viitattu 13.3.2022.

———. 2022e. *Volvon tarjoaman langattoman verkon ulkoisen osoitteen analyysi.* Saatavilla WWW-muodossa, https://drive.google.com/file/d/1wi20eookbt-ng1nqVgFDfrSpyAfPjZFz/view?usp=sharing, viitattu 13.3.2022.

Pasanen, Mauno. 2022f. *VW GTEn etähallintasovelluksen liikennekaappaus.* Saatavilla WWW-muodossa, https://drive.google.com/file/d/1zHSvlPVwMZLfYxNYDLuAZUZlKHMYhl4n/view?usp=sharing, viitattu 30.4.2022.

Pham, Minh, ja Kaiqi Xiong. 2021. "A survey on security attacks and defense techniques for connected and autonomous vehicles". *Computers & Security* 109:102269. ISSN: 0167-4048. https://doi.org/10.1016/j.cose.2021.102269.

Puliafito, Carlo, Enzo Mingozzi, Francesco Longo, Antonio Puliafito ja Omer Rana. 2019. "Fog Computing for the Internet of Things: A Survey". *ACM Trans. Internet Technol.* (New York, NY, USA) 19, numero 2 (huhtikuu). ISSN: 1533-5399. https://doi.org/10.1145/3301443.

Rana, K. 2011. "Classification of SQL injection attacks and using encryption as A countermeasure". Teoksessa *International Journal of Advanced Research in Computer Science.* https://www.proquest.com/scholarly-journals/classification-sql-injection-attacks-using/docview/1443705484/se-2.

ReportLinker. 2021. *Edge Computing Market - Growth, Trends, COVID-19 Impact, and Forecasts (2021 - 2026).* Saatavilla WWW-muodossa, https://www.reportlinker.com/p06062848/Edge-Computing-Market-Growth-Trends-COVID-19-Impact-and-Forecasts.html, viitattu 1.4.2021.

Roman, Rodrigo, Javier Lopez ja Masahiro Mambo. 2018. "Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges". *Future Generation Computer Systems* 78:680–698. ISSN: 0167-739X. https://doi.org/10.1016/j.future.2016.11.009.

Ronen, Eyal, Adi Shamir, Achi-Or Weingarten ja Colin O'Flynn. 2017. "IoT Goes Nuclear: Creating a ZigBee Chain Reaction". Teoksessa *2017 IEEE Symposium on Security and Privacy (SP),* 195–212. https://doi.org/10.1109/SP.2017.14.

Roy, Aditi, Nasir Memon, Julian Togelius ja Arun Ross. 2018. "Evolutionary Methods for Generating Synthetic MasterPrint Templates: Dictionary Attack in Fingerprint Recognition". Teoksessa *2018 International Conference on Biometrics (ICB),* 39–46. https://doi.org/10.1109/ICB2018.2018.00017.

SAE International. 2021. *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles.* Saatavilla WWW-muodossa, https://www.sae.org/standards/content/j3016_202104/, viitattu 29.1.2022.

Samy, Ahmed, Haining Yu ja Hongli Zhang. 2020. "Fog-Based Attack Detection Framework for Internet of Things Using Deep Learning". *IEEE Access* 8:74571–74585. https://doi.org/10.1109/ACCESS.2020.2988854.

Schroff, Florian, Dmitry Kalenichenko ja James Philbin. 2015. "FaceNet: A unified embedding for face recognition and clustering". Teoksessa *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR),* 815–823. https://doi.org/10.1109/CVPR.2015.7298682.

Selvaraj, Jayaprakash, Gökçen Yılmaz Dayanıklı, Neelam Prabhu Gaunkar, David Ware, Ryan M. Gerdes ja Mani Mina. 2018. "Electromagnetic Induction Attacks Against Embedded Systems". Teoksessa *Proceedings of the 2018 on Asia Conference on Computer and Communications Security,* 499–510. ASIACCS '18. Incheon, Republic of Korea: Association for Computing Machinery. ISBN: 9781450355766. https://doi.org/10.1145/3196494.3196556.

Sengupta, Jayasree, Sushmita Ruj ja Sipra Das Bit. 2020. "A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT". *Journal of Network and Computer Applications* 149:102481. ISSN: 1084-8045. https://doi.org/10.1016/j.jnca.2019.102481.

Shehab, Mohamed, ja Fadi Mohsen. 2014. "Securing OAuth Implementations in Smart Phones". Teoksessa *Proceedings of the 4th ACM Conference on Data and Application Security and Privacy,* 167–170. CODASPY '14. San Antonio, Texas, USA: Association for Computing Machinery. ISBN: 9781450322782. https://doi.org/10.1145/2557547.2557588.

Society of Automotive Engineers, SAE. 2016. *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems.* Saatavilla WWW-muodossa, https://www.sae.org/standards/content/j3061_201601/, viitattu 12.2.2022.

Sun, San-Tsai, ja Konstantin Beznosov. 2012. “The Devil is in the (Implementation) Details: An Empirical Analysis of OAuth SSO Systems”. Teoksessa *Proceedings of the 2012 ACM Conference on Computer and Communications Security,* 378–390. CCS ’12. Raleigh, North Carolina, USA: Association for Computing Machinery. ISBN: 9781450316514. https://doi.org/10.1145/2382196.2382238.

Taosoftware Co., Ltd. 2015. *tPacketCapture.* Saatavilla Android sovelluskaupasta, https://play.google.com/store/apps/details?id=jp.co.taosoftware.android.packetcapture&hl=fi&gl=US, viitattu 12.2.2022.

Tietoarkisto. 2022. *Tunnisteellisuus ja anonymisointi.* Saatavilla WWW-muodossa, https://www.fsd.tuni.fi/fi/palvelut/aineistonhallinta/tunnisteellisuus-ja-anonymisointi/, viitattu 8.1.2022.

West, Darrell M. 2016. “Moving forward: self-driving vehicles in China, Europe, Japan, Korea, and the United States”. *Center for Technology Innovation at Brookings: Washington, DC, USA,* https://www.academia.edu/download/52649783/DriverlessCars.pdf.

Wireshark.org. 2022. *Wireshark.* Saatavilla www-muodossa, https://www.wireshark.org/, viitattu 12.2.2022.

Volkswagen. 2022a. *we Connect.* Saatavilla WWW-muodossa, https://www.volkswagen.fi/fi/innovaatiot-ja-teknologia/yhdistettavyys/we-connect.html, viitattu 29.1.2022.

———. 2022b. *Volkswagen introduces Over-the-Air Updates for all ID. models.* Saatavilla WWW-muodossa, https://www.volkswagen-newsroom.com/en/press-releases/volkswagen-introduces-over-the-air-updates-for-all-id-models-7497, viitattu 29.1.2022.

Volkswagen AG. 2022. *Tietosuojalauseke koskien Volkswagen AG:n online-mobiilipalveluiden (Car-Net ja We Connect) käyttämistä ja tietojen keräämistä anonymisoidun tietokannan kokoamiseksi automatisoidun ajamisen kehittämistä varten osassa III.* Saatavilla WWW-muodossa, https://consent.vwgroup.io/consent/v1/texts/CarNet/fi/fi/dataprivacy/latest/pdf, viitattu 25.9.2022.

Volvo. 2022a. *Downloading and updating apps.* Saatavilla WWW-muodossa, https://www.volvocars.com/uk/support/topics/in-car-apps/manage-apps/downloading-and-updating-apps, viitattu 29.1.2022.

———. 2022b. *Infotainment and Digital Consumer Experience.* Saatavilla WWW-muodossa, https://group.volvocars.com/company/innovation/android, viitattu 29.1.2022.

———. 2022c. *The Volvo Cars app.* Saatavilla WWW-muodossa, https://www.volvocars.com/uk/support/topics/connected-services/the-volvo-cars-app, viitattu 29.1.2022.

Volvo Cars. 2022. *Tietosuojailmoitus – Volvo Cars -sovellus.* Saatavilla WWW-muodossa, https://www.volvocars.com/fi/legal/privacy/privacy-voc/2022.87.0, viitattu 25.9.2022.

Wu, Dong-Jie, Ching-Hao Mao, Te-En Wei, Hahn-Ming Lee ja Kuo-Ping Wu. 2012. "DroidMat: Android Malware Detection through Manifest and API Calls Tracing". Teoksessa *2012 Seventh Asia Joint Conference on Information Security,* 62–69. https://doi.org/10.1109/AsiaJCIS.2012.18.

Xiao, Yinhao, Yizhen Jia, Chunchi Liu, Xiuzhen Cheng, Jiguo Yu ja Weifeng Lv. 2019. "Edge Computing Security: State of the Art and Challenges". *Proceedings of the IEEE* 107 (8): 1608–1631. https://doi.org/10.1109/JPROC.2019.2918437.

Yousefpour, Ashkan, Caleb Fung, Tam Nguyen, Krishna Kadiyala, Fatemeh Jalali, Amirreza Niakanlahiji, Jian Kong ja Jason P. Jue. 2019. "All one needs to know about fog computing and related edge computing paradigms: A complete survey". *Journal of Systems Architecture* 98:289–330. ISSN: 1383-7621. https://doi.org/10.1016/j.sysarc.2019.02.009.

Zaabi, Abdulla O. Al, Chan Yeob Yeun ja Ernesto Damiani. 2019. "Autonomous Vehicle Security: Conceptual Model". Teoksessa *2019 IEEE Transportation Electrification Conference and Expo, Asia-Pacific (ITEC Asia-Pacific),* 1–5. https://doi.org/10.1109/ITEC-AP.2019.8903691.

Zhang, Jiale, Bing Chen, Yanchao Zhao, Xiang Cheng ja Feng Hu. 2018. "Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues". *IEEE Access* 6:18209–18237. https://doi.org/10.1109/ACCESS.2018.2820162.

Zhou, Xiaoyong, Soteris Demetriou, Dongjing He, Muhammad Naveed, Xiaorui Pan, Xiao-Feng Wang, Carl A. Gunter ja Klara Nahrstedt. 2013. “Identity, Location, Disease and More: Inferring Your Secrets from Android Public Resources”. Teoksessa *Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security,* 1017–1028. CCS ’13. Berlin, Germany: Association for Computing Machinery. ISBN: 9781450324779. https://doi.org/10.1145/2508859.2516661.

Zolotukhin, Mikhail, Timo Hämäläinen, Tero Kokkonen ja Jarmo Siltanen. 2016. “Increasing web service availability by detecting application-layer DDoS attacks in encrypted traffic”. Teoksessa *2016 23rd International Conference on Telecommunications (ICT),* 1–6. https://doi.org/10.1109/ICT.2016.7500408.

Örs, Sıddıka Berna, Elisabeth Oswald ja Bart Preneel. 2003. “Power-analysis attacks on an FPGA–first experimental results”. Teoksessa *International Workshop on Cryptographic Hardware and Embedded Systems,* 35–50. Springer. ISBN: 978-3-540-45238-6. https://doi.org/10.1007/978-3-540-45238-6_4.

Liitteet

A Reunalaskennan käsitteistöä

(Pasanen 2021)

- **Mobiilipilvilaskenta (MCC)** määritellään Yousefpour ym. (2019) mukaan infrastruktuuriksi, jossa sekä tietojen tallennus että tietojenkäsittely tapahtuvat mobiililaitteen ulkopuolella, mikä tuo mobiilisovelluksia paitsi älypuhelinten käyttäjille myös paljon laajemmalle joukolle matkaviestintilaajista. Tutkimuksen mukaan Yhdysvaltain standardoimisinstituutti NIST (National Institute of Standards and Technology) laajentaa tämän määritelmän koskemaan myös mobiililaitteita: pilvilaskenta on esineiden internetin laitteiden, mobiililaitteiden ja pilvipalvelujen välinen synergia, joka mahdollistaa data- ja prosessori-intensiiviset sovellukset esineiden internetin -ympäristöissä. Mobiilipilvipalvelun sovellukset sisältävät muun muassa joukkorahoituksen, terveydenhuollon, tehtävien siirron ja sensoritietojen käsittelyn (kuten optisen merkkien tunnistuksen ja kuvankäsittelyn). (Yousefpour ym. (2019).) Mobiilipilvipalvelu on Naha ym. (2018) mukaan yleensä kevyt reunapilvipalvelin, joka on sijoitettu verkon reunaan.
- **Mobiili-ad-hoc-laskenta (MACC)**. Mobiilipilvilaskennan yleisestä luonteesta huolimatta tämä laskentamalli ei aina sovellu skenaarioihin, joissa puuttuu infrastruktuuri, tai keskitetty pilvi. Ad-hoc-mobiiliverkko on verkon hajautetuin muoto ja koostuu solmuista, jotka muodostavat väliaikaisen ja dynaamisen verkon reititys- ja siirtoprotokollien avulla. Ad -hoc -mobiiliverkossa olevat mobiililaitteet muodostavat erittäin dynaamisen verkkotopologian. Laitteiden muodostama verkko on erittäin dynaaminen, ja sen on sopeuduttava jatkuvasti liittyviin ja poistuviin laitteisiin. Ad hoc -laitteet voivat muodostaa väliaikaisia pilviä, joita voidaan käyttää verkottumiseen, tallennukseen ja tietojenkäsittelyyn, esimerkiksi ryhmän suoraan videon toistoon ja miehittämättömien ajoneuvojen järjestelmiin. (Yousefpour ym. (2019).)
- **Monipääsyreunalaskenta (Multi-access Edge Computing, MEC)** tai aiemmin **mobiilireunalaskenta (Mobile-Edge-Computing)** on mobiililaskennan laajennus reunalaskennan kautta. Telealan europpalainen standardoimisjärjestö ETSI (European Te-

lecommunications Standards Institute) määrittelee monipääsyreunalaskennan alustaksi, joka tarjoaa informaatioteknologia- ja pilvipalveluominaisuuksia 4G ja 5G -pääsyverkossa (RAN) matkapuhelintilaajien välittömässä läheisyydessä. (Yousefpour ym. (2019).) Monipääsyreunalaskenta ehdottaakin Naha ym. (2018) mukaan tietojenkäsittelyn ja tallennuksen rinnakkaista sijoittamista matkapuhelinverkkojen tukiasemille. Monipääsyreunalaskentaa kutsuttiin aiemmin ”mobiilireunalaskennaksi”, mutta käsitettä on laajennettu kattamaan laajempi valikoima sovelluksia mobiililaitekohtaisten tehtävien lisäksi. Esimerkkejä monipääsyreunalaskentasovelluksista ovat videoanalytiikka, yhdistetyt ajoneuvot, terveydentilan seuranta ja lisätty todellisuus. (Yousefpour ym. (2019).)

- **Reunapilvipalvelin (minipilvi, cloudlet)** on luotettava ja resurssirikas tietokone tai tietokonejoukko, jolla on vahva Internet-yhteys, ja jota lähellä olevat mobiililaitteet hyödyntävät. Reunapilvipalvelimet ovat pieniä laskentakeskuksia, jotka ovat tyypillisesti yhden verkkohypyn päässä mobiililaitteista. (Yousefpour ym. (2019).)
- **Sumulaskenta (Fog Computing, FC)**, on Bonomi ym. (2012), mukaan erittäin virtualisoitu alusta, joka tarjoaa laskenta-, tallennus- ja verkkopalveluja esineiden internetin laitteiden ja perinteisten pilvipalvelutietokeskusten välillä. Sumulaskentaa pidetään useasti synonyyminä reunalaskennalle. Vaikka sumu- ja reunalaskenta siirtävät laskennan ja tallennuksen verkon reunaan ja lähemmäs päätelaitteita, käsitteet eivät ole identtisiä. Yousefpour ym. (2019) mukaan OpenFog konsortio itse asiassa toteaa, että reunalaskentaa kutsutaan usein virheellisesti sumulaskennaksi. OpenFog-konsortio tekee eron siitä, että sumulaskenta on hierarkkinen ja se tarjoaa tietojenkäsittelyn, verkottumisen, tallennuksen, hallinnan ja nopeuttamisen missä tahansa pilvestä esineisiin, kun reunalaskenta taas rajoittuu laskemiseen yhden verkkohypyn päässä laitteista. Sumulaskennan arkkitehtuuria kuvataan hyvin pilveä vastaavaksi, laajentaen pilvipalvelut verkon reunalle. Sumusolmut ottavat käyttöön ja tarjoavat samantyyppisiä XaaS-palveluja kuin pilvipalvelut. Erona pilvilaskentaan sumulaskennan arkkitehtuuri käyttää lisäksi yhtä tai useampaa yhteistyössä toimivaa loppukäyttäjäasiakasta tai läheisen organisaation reunalaitetta, jotka suorittavat huomattavan määrän viestintä-, ohjaus-, määritys-, mittaus- ja hallintapalveluita. (Mahmood (2018, 5).) Arkkitehtuurimallia selventää Puliafito ym. (2019) sivun 8 kuvio 2 sumulaskennan hierarkkiasta, jossa sumusolmut ovat sekä hajautettuna että yhdistettynä esineiden internetin laiteta-

solta ydinverkkoon saakka.

- **Usvalaskenta (Mist Computing)** kuvaa hajautettua tietojenkäsittelyä itse esineiden internetin laitteissa, ja sitä on ehdotettu ajatellen itsetietoisia ja autonomisia järjestelmiä. Usvalaskenta voidaan nähdä ensimmäisenä laskentapaikkana esineiden internetin-sumupilven jatkumossa, ja sitä voidaan epävirallisesti kutsua termeillä ”esineiden internetin-tietojenkäsittely” tai ”laitteiden tietojenkäsittely”. Laite voi olla esimerkiksi puettava, mobiililaite, älykello tai älykäs jääkaappi. (Yousefpour ym. (2019).)
- **Reunalaskenta (Edge Computing, EC)** sijaitsee verkon reunalla lähellä esineiden internetin laitteita. Yhden määritelmän mukaan reunalaskenta ei ole itse laitteissa, vaan yhden verkkohypyn päässä tapahtuvaa laskentaa. OpenEdge Computing määrittelee reunalaskennan toiminnaksi, joka suoritetaan verkon laidalla pienissä lähellä käyttäjiä sijaitsevissa datakeskuksissa. (Yousefpour ym. (2019).) NIST määrittää käsitteen päätelaitteet ja niiden käyttäjät kattavaksi verkkokerrokseksi (esineiden internet-verkko), joka tarjoaa paikallisen laskentatoiminnon esimerkiksi sensorissa, mittauslaitteessa tai muissa verkossa käytettävissä laitteissa (Iorga ym. 2018). Esimerkkeinä erilaisesta reunan tulkinnasta Naha ym. (2018) antaa 1) reunapilvipalvelimen sijainnin mobiilisovelluksen ja perinteisen pilven välissä, kun taas 2) esineiden internetin yhdyskäytävä on sensorin ja perinteisen pilvipalvelun välinen reuna.
- **Kastelaskenta (Dew Computing, DC)** yhdistää pilvipalvelun pääkonseptin päätelaitteiden ominaisuuksiin. Sitä käytetään parantamaan loppukäyttäjän käyttökokemusta verrattuna pilvipalveluihin. Naha ym. (2018) mukaan kastelaskenta sijaitsee pilven ja sumutietokoneiden ympäristössä, perustuu mikropalveluihin, ja palvelee sensoreita, tabletteja ja matkapuhelimia, jotka ovat saumattomasti yhdistetty verkkoon ad-hoc-pohjaisilla ratkaisuilla. Esimerkiksi liikennevalojen välissä sijaitsevat älykkään liikenteenohjausjärjestelmän tiedonkeruu- ja käsittelylaitteet voivat luoda liikennetilanteen kokonaiskuvan, ja välittää sen autoille esimerkiksi polttoainevalinnan optimoimiseksi.
- **Sumu-kastelaskenta (Fog-Dew Computing, FDC)**. Sumu-kastelaskennan arkkitehtuurissa esineiden internetin laitteilla ei tarvitse olla aktiivista Internet-yhteyttä, kun ne ovat yhteydessä yhteisöpalvelimelle. Yhteisöpalvelin on vuorovaikutuksessa pilven kanssa ja vastaa palvelujen tarjoamisesta esineiden internetin laitteille. Esimerkkeinä sumu-kastelaskennasta on Google Drive ja Dropbox, joissa käyttäjät voivat poistaa,

luoda ja päivittää tiedostoja ja kansioita ilman Internet-yhteyttä, ja synkronoida ne sitten, kun laite on yhdistetty Internettiin. (Naha ym. (2018).)