Fabian Lindblom

KOTKANSAAREN IOT-LAITTEIDEN KARTOITTAMINEN JA RISKIANALYYSI

Opinnäytetyö

Tekniikan ammattikorkeakoulututkinto

Kyberturvallisuuden koulutus

2024

Kaakkois-Suomen ammattikorkeakoulu

Kaakkois-Suomen ammattikorkeakoulu

Tutkintonimike	Insinööri (AMK)
Tekijä/Tekijät	Fabian Lindblom
Työn nimi	Kotkansaaren IoT-laitteiden kartoittaminen ja riskianalyysi
Toimeksiantaja	Kaakkois-Suomen ammattikorkeakoulu
Vuosi	2024
Sivut	80 sivua
Työn ohjaaja(t)	Vesa Kankare

TIIVISTELMÄ

Kyberturvallisuus on monimuotoista, mikä johtaa helposti siihen, että kaikkia siihen liittyviä seikkoja ei välttämättä osata ottaa huomioon yhtä tarkasti. Hyvä esimerkki tästä on esimerkiksi se, että IoT-laitteiden kyberturvallisuustilannetta ei olla kartoitettu tarpeeksi kaikkien tiedonsiirtoteknologioiden osalta. Näitä vähemmän tutkittuja teknologioita on tärkeää tutkia siksi, että tällä tavoin voidaan tuoda esille aikaisemmin tuntemattomia kyberturvallisuusongelmia.

Tutkimuksessa kartoitettiin Wardrivingin avulla Kotkansaarella sijaitsevia IoT-laitteita ja lopuksi niistä tehtiin riskianalyysiä. Tutkimuksen toimeksiantajana toimi Kaakkois-Suomen ammattikorkeakoulu.

Tutkimuksessa suoritettiin Wardriving-kartoitusta, joka kohdistui kyberturvallisuuden kannalta kaikista kiinnostavimpiin kohteisiin, kuten teollisuuteen ja muuhun kriittiseen infrastruktuuriin. Lisäksi Kotkansaarta pitkin ajeltiin satunnaisotannalla, jotta saataisiin mahdollisimman kattava kuva nykyisestä kyberturvallisuustilanteesta.

Tutkimus toteutettiin laadullisena. Tutkimuksen lähestymistapa perustuu tapaustutkimukseen, sillä tapaustutkimus mahdollistaa kattavan ja yksityiskohtaisen tarkastelun tutkittavasta ilmiöstä. Tutkimuksesta kerättiin kattava määrä sekundääriaineistoa primääriaineiston tueksi. Lisäksi aineistoa kerättiin tutkimalla löydettyjä laitteita myös paikan päällä.

Tulosten avulla löydettiin massiivinen määrä erilaisia IoT-laitteita. Moni näistä laitteista oli haavoittuvainen erilaisille hyökkäyksille. Teoreettisten uhkien lisäksi löydettiin myös paljon konkreettisia todisteita siitä, miten eri tasoiset uhat ovatkin usein todistettu toimiviksi myös reaalimaailman tilanteissa. Osa löydetyistä uhkista koskee siis tälläkin hetkellä Kotkansaaren asukkaita.

Tämä opinnäytetyö tuo esille aikaisemmin tuntemattomia uhkia, joiden esilletuomisella voi olla merkittävä vaikutus kyberturvallisuuden tasoon. Lisäksi tutkimus luo pohjaa jatkotutkimuksille ja kehitystoimille kyberturvallisuuden alalla.

Asiasanat: kyberturvallisuus, wardriving, IoT, ohjelmistoradio, riskianalyysi

South-Eastern Finland University of Applied Sciences

Degree title	Bachelor of Engineering
Author	Fabian Lindblom
Thesis title	Mapping and risk analysis of IoT devices in Kotkansaari
Commissioned by	South-Eastern Finland University of Applied Sciences
Time	2024
Pages	80 pages
Supervisor	Vesa Kankare

ABSTRACT

Cybersecurity is a diverse concept, which easily leads to a situation where not all related aspects are equally considered. A good example of this is the fact that the cybersecurity status of IoT devices has not been adequately assessed for all data transmission technologies. It is important to study these less researched technologies to reveal previously unknown cybersecurity issues.

The study utilized Wardriving to map IoT devices on Kotkansaari and ultimately perform a risk analysis on them. Wardriving mapping focused on the most interesting targets with respect to cybersecurity, such as industrial areas and other critical infrastructure. Additionally, random driving routes were taken to acquire the most comprehensive picture of the current cybersecurity situation.

The study was qualitative and it was based on case study. A considerable amount of secondary data was collected to support the primary data. The secondary data primarily comprised a wide variety of previous studies, while the primary data was exclusively collected through wardriving. Additionally, data was collected by examining the discovered devices on-site.

The results revealed a massive number of different IoT devices, many of which were vulnerable to various attacks. In addition to theoretical threats, many concrete pieces of evidence were found showing how threats of different levels are often realized in real-world situations. Some of the identified threats currently affect the residents of Kotkansaari.

This thesis highlights previously unknown threats, the exposure of which may have a significant impact on the level of cybersecurity. Additionally, the study lays the groundwork for further research and development in the field of cybersecurity.

Keywords: cybersecurity, wardriving, IoT, Software-Defined radio, risk analysis

SISÄLLYS

1 JOHDANTO

Nykymaailma siirtyy jatkuvasti kohti entistäkin älykkäämpää ja kytketympää tulevaisuutta, missä esineiden internet (IoT) on keskeisessä asemassa. Tämä muutos näkyy monilla elämänalueilla, kuten terveydenhuollossa, liikenteessä, teollisuudessa ja kotona. IoT:n etuja ovat muun muassa tehokkuuden parantaminen, mukavuuden lisääminen ja innovaatioiden mahdollistaminen. Esineiden internet tuo siis monia hyötyjä, mutta samalla se myös lisää tietoturvahaasteita.

Yhä useammat laitteet keräävät ja jakavat tietoa verkossa, mikä luo uusia mahdollisuuksia tietomurroille ja väärinkäytöksille. Yksi keskeisimmistä haasteista on laitteiden heikko kyberturvallisuuden taso, joka voi johtua puutteellisista salausmenetelmistä, haavoittuvuuksista ohjelmistossa tai laitteiden vanhentuneista päivityksistä. Näiden ongelmien havaitseminen ja tietoturvaongelmien mitigointi on siksi tärkeää.

Wardriving tarjoaa kätevän ratkaisun IoT-laitteiden tutkimiseen ja mahdollisten tietoturvaongelmien paljastamiseen. Wardrivingin avulla voidaan kartoittaa IoT-laitteiden levinneisyyttä, havaita heikosti suojattuja laitteita ja tunnistaa ongelmia ennen mahdollisia väärinkäytöksiä. Näistä syistä Wardriving on valittu tutkimuksen pääasialliseksi tavaksi kerätä tietoja ja selvittää kyberturvallisuuden nykytasoa.

2 TUTKIMUSASETELMA

Tämän tutkimuksen keskeisenä tavoitteena on syventyä IoT-laitteiden kyberturvallisuustilanteeseen. Lisäksi tutkitaan sitä, että voidaanko näistä laitteista kerätä tietoa Wardriving-tekniikan avulla. Wardrivingin käyttö IoT-laitteiden tietojen keräämisessä on kiinnostava näkökulma, koska se mahdollistaa laajemman katsauksen laitteiden turvallisuustilanteeseen. Tällainen tutkimus avaisi uusia mahdollisuuksia ymmärtää ja torjua IoT-laitteiden kyberturvallisuuteen liittyviä riskejä ja haavoittuvuuksia.

Wardrivingia on pääasiassa sovellettu Wi-Fi-verkkojen havainnointiin, mutta sen soveltamista esimerkiksi Bluetooth- ja muita ISM-radiotaajuuksia

käyttävien laitteiden havaitsemiseen on ollut vähäisempää. Varsinainen tutkimusongelma on siis se, että IoT-laitteiden kyberturvallisuustilannetta ei olla kartoitettu tarpeeksi kaikkien tiedonsiirtoteknologioiden osalta.

2.1 Tutkimuskysymykset

Edellä mainitusta ongelmanasettelusta johdetaan seuraavat tutkimuskysymykset:

1. Voidaanko IoT-laitteiden dataa kerätä tutkimuksessa käytetyllä laitteistolla Wardriving-tekniikkaa hyödyntäen?

2. Miten erilaisten Bluetooth-teknologian datapakettien ja ISM-radiotaajuuksilla toimivien pakettien, sisältö vaihtelee ja miten ne voivat tukea tutkimusta?

3. Miten tutkimuksen tuloksia voidaan käyttää kyberturvallisuuden kehittämiseen?

Tutkimuksen on määrä vastata näihin tutkimuskysymyksiin analysoimalla kerättyä dataa ja tuottamalla selkeitä tuloksia ja johtopäätöksiä.

2.2 Tutkimusote

Tämän tutkimuksen lähestymistapa perustuu tapaustutkimukseen, sillä tapaustutkimus mahdollistaa kattavan ja yksityiskohtaisen tarkastelun tutkittavasta ilmiöstä. Tämä tutkimustyyppi sopii erityisesti silloin, kun tutkitaan "miksi-” ja "miten"-kysymyksiä reaalimaailman tilanteissa (Gerring 2004).

Tapaustutkimus mahdollistaa myös tutkimuksen suorittamisen todellisissa ympäristöissä, jolloin voidaan havainnoida IoT-laitteiden käyttöä ja altistumista erilaisille tietoturvariskeille. Lisäksi tapaustutkimus tuo monipuolisen lähestymistavan tutkimukseen, jossa voidaan ottaa huomioon erilaisia tekijöitä, kuten IoT-laitteiden fyysinen sijainti, haavoittuvuudet ja käytetyt protokollat.

Tutkimus pohjautuu laajaan teoreettiseen viitekehykseen IoT:hen, tietoturvaan, laitteiston toimintaan, eri ohjelmistoihin ja Wardrivingiin liittyen.

Tutkimuksen avulla pyritään tarjoamaan konkreettinen näkökulma IoT-laitteiden tietoturvan ymmärtämiseen ja parantamiseen.

2.3 Aineiston keruu ja analyysi

Tutkimus aloitetaan keräämällä sekundääriaineistoa tutkittavasta kohteesta. Sekundääriaineisto koostuu aineistosta, joka on jo saatavilla aiheesta (Kananen 2008). Kerättävää aineistoa ovat mm. tieto mahdollisesti kiinnostavista kohteista, jonka perusteella luodaan ajettava reitti, RTL-SDR-ohjelmistoradion toiminta ja Bluetooth-vastaanottimen soveltuvuus IoT-laitteiden tutkintaan.

Tutkimuksen tuloksia esitetään hyödyntämällä tilastoja ja grafiikkaa. Graafisella analyysillä voidaan esittää kerättyjen tilastojen tuloksia ja luodut graafit saattavat paljastaa suuren datamäärän poikkeavuuksia, jotka taas voivat antaa mahdollisia vastauksia tutkimuskysymyksille (Lähdesmäki ym. 2009).

Tapaustutkimuksen tuloksia yhdistetään myöhemmin sekundääriaineiston tietolähteisiin. Näin voidaan esimerkiksi verrata tutkimuksessa kerättyjen tilastojen tuloksia jo aikaisempaan tietoon siitä, miten IoT-laitteet käyttävät tutkittavia protokollia. Tällä tavoin voidaan selvitää esimerkiksi, että onko tietojen keruu ollut onnistunutta ja onko RTL-SDR- ja Bluetooth-vastaanottimilla ylipäätään mahdollista kerätä tutkimuksen aiheena olevaa dataa.

Datan keräämisen luotettavuutta voidaan arvioida sen perusteella, että ovatko tulokset realistisia. Toisin sanoen, jos IoT-laitteita havaitaan esimerkiksi paljon tietyissä paikoissa, missä niitä ei sekundääriaineiston mukaan pitäisi olla ollenkaan, voidaan päätellä, että datan luotettavuudessa saattaa olla ongelmia.

2.4 Kerättävän primääriaineiston määrittely

IoT-laitteiden käyttämien protokollien moninaisuus lisää haasteita. Eri valmistajat hyödyntävät erilaisia protokollia ja standardeja (Madakam ym. 2015). Tutkimuksen suorittamiseksi tehokkaasti ja ilman ylimääräistä

monimutkaisuutta tiettyjä protokollia ja taajuusalueita on rajattu. Nämä rajaukset pyrkivät parantamaan tutkimuksen selkeyttä ja keskittymään olennaiseen. Rajauksiin kuuluvat kaksi seuraavaa tekijää:

Vain Bluetooth Low Energy -paketit. Tutkimus keskittyy pääasiassa Bluetooth Low Energy -paketteihin. Mahdollisesti kaikki paketit, jotka löytyvät, otetaan kuitenkin huomioon, mutta niitä ei välttämättä käsitellä erikseen.

Vain RTL-SDR-vastaanottimen taajuudet 315 MHz, 433 Mhz, 868 Mhz ja 915 MHz. Tutkimus rajoittuu RTL-SDR-vastaanottimen käyttöön taajuuksilla 315 MHz, 433 Mhz, 868 Mhz ja 915 MHz. Tämä rajaus perustuu siihen, että nämä taajuudet ovat käytössä myös Rtl_433-ohjelmistossa (Github s.a.). Näin ollen voidaan olettaa, että suurin osa IoT-laitteista toimii mainituilla taajuuksilla. Toinen syy rajaukseen on se, että käytetty ohjelmisto ei todennäköisesti tue muilla taajuusalueilla toimivia laitteita, vaikka ohjelmisto pystyisi ainakin teoriassa vastaanottamaan myös muita taajuuksia.

Kokeilemalla voidaan todeta datan keräämisen toimivuus tai sen toimimattomuus. Tämän vuoksi testausjärjestely on kuvattava yksityiskohtaisesti, ja ennen testausta on määriteltävä odotettu lopputulos onnistuneelle testaukselle. Tämä varmistaa tutkimuksen luotettavuuden.

Tutkimuksen lopussa kerättyä dataa analysoidaan objektiivisesti siten, että sen voidaan tulkita olevan sekundääriaineiston kanssa paikkaansa pitävä. Tämä tapahtuu vertaamalla tutkimuksessa käytettävien laitteiden antamia tuloksia sekundääriaineistoon. Esimerkiksi jatkuvan sähkömagneettisen tai muun lähteen häiriön aiheuttama data voidaan poistaa analysoitavasta datasta vertaamalla kerättyä dataa aikaisempaan tietoon aiheesta. Tämän lisäksi laitteita tutkitaan myös paikan päällä, koska se konkretisoi tutkimusta ja mahdollistaa lisätietojen keräämisen laitteista.

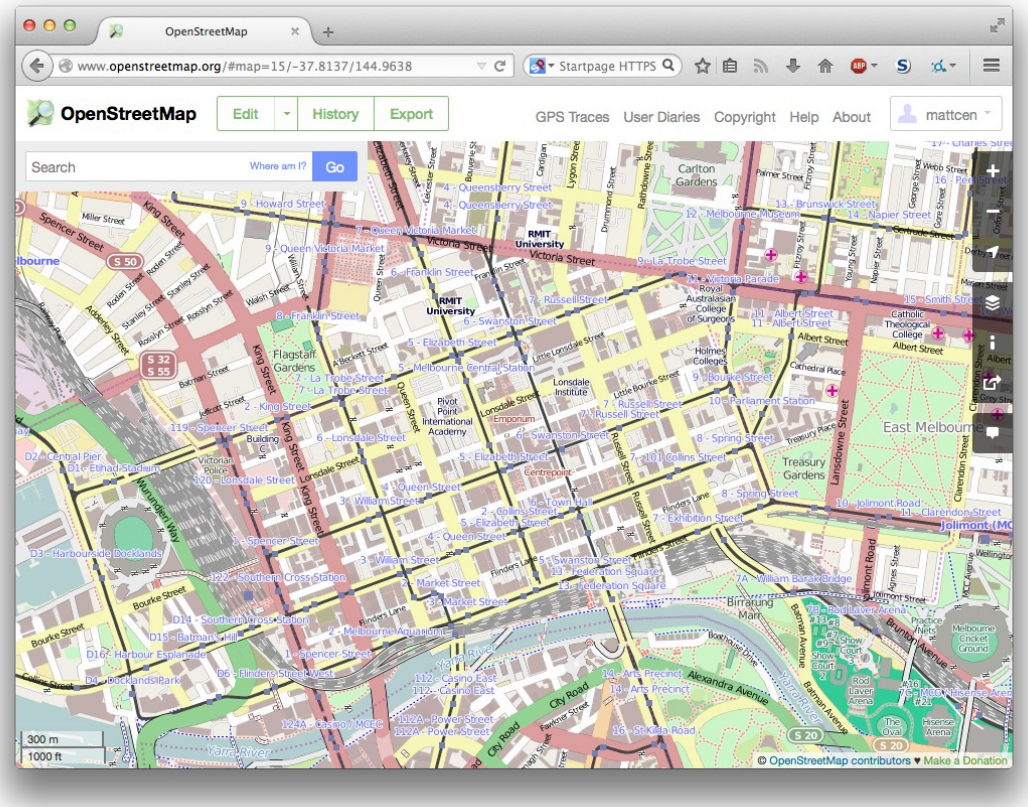
2.5 Tavoite

Tutkimuksen päämääränä on kerätä mielenkiintoista tietoa IoT-laitteiden kyberturvallisuustilanteesta sekä tuoda ilmi mahdollisia ongelmia niihin liittyen. Tutkimuksen tavoitteena on myös selvittää, että voidaanko SDR- ja Bluetooth-

teknologioiden avulla kerätä tietoja IoT-laitteista Wardriving-tekniikkaa hyödyntäen. Lisäksi tutkimuksen loppuvaiheessa tehdään riskianalyysiä koskien löydettyjä IoT-laitteita.

Ensimmäinen osa tutkimusta on toimivan laitteiston rakentaminen määrätyn datan keräämistä varten. Kun laitteisto on valmis, suunnitellaan henkilöautolla ajettava reitti. Reitti suunnitellaan mahdollisimman tehokkaaksi datan keräämisen näkökulmasta. Reitti siis valitaan kulkevaksi paikoista, joissa on todennäköisimmin kiinnostavia IoT-laitteita. Tämä toteutetaan tarkastelemalla karttapalveluja, kuten esimerkiksi Google Mapsia. Lisäksi on tarpeen määritellä sekundääriaineiston perusteella, mitkä kohteet voisivat olla tutkimuksen kannalta kiinnostavia, jotta reitti voidaan suunnitella niiden ympärille.

Näiden toimenpiteiden jälkeen yhdistetään sekundääriaineiston avulla luotu ja kokeilemalla toimivaksi havaittu laitteisto ohjelmistoon. Ohjelmiston on määrä koostua mahdollisimman varmasta ja laajasta toiminnallisuuden kirjosta, joka vastaa tutkimuksen tarpeita. Lopuksi yhdistetty data visualisoidaan ja selitetään niin, että tuloksia voidaan hyödyntää reaalimaailman skenaarioissa (kuva 1).



Kuva 1. Esimerkkikuva OpenStreemapin avulla luodusta kartasta (mattcen.github.io s.a.)

Tutkimuksen yksi tärkeimmistä tavoitteista on saada dataa, josta voi olla hyötyä kyberturvallisuudelle ja sen jatkokehitykselle. Tavoitteen voidaan katsoa onnistuneeksi, jos tuloksena saadaan dataa IoT-laitteista tässä tutkimuksessa käsitellyllä tavalla.

Tutkimuksen tuloksia voidaan hyödyntää lisäksi opetuksellisessa tarkoituksessa tarjoamalla tietoa ja käytännön esimerkkejä IoT-laitteiden havainnoinnista sekä niiden tietoturvaan liittyvistä haasteista. Tämä antaisi toimeksiantajalle mahdollisuuden käyttää tutkimusta opetuksellisissa tapahtumissa esimerkiksi koulutusohjelmissa, seminaareissa tai koulutustilaisuuksissa, joissa käsitellään tietoturvaa, langattomia verkkoteknologioita tai IoT-laitteiden käyttöä ja niiden turvallisuutta.

3 TEOREETTINEN VIITEKEHYS

3.1 Wardriving

Wardriving on termi, joka viittaa liikkumiseen fyysisessä ympäristössä tarkoituksena tunnistaa ja kartoittaa langattomia verkkoyhteyksiä. Alun perin

Wardriving keskittyi Wi-Fi-verkkoihin, mutta on laajentunut koskemaan monenlaisia langattomia laitteita, kuten IoT-laitteita. Wardrivingin avulla pyritään havaitsemaan ja analysoimaan langattomia signaaleja, tunnistamaan verkkoihin liittyviä haavoittuvuuksia ja selvittämään mahdollisia tietoturvauhkia (What is Wardriving? s.a.).

Tämän tutkimuksen tulokset on määrä saada Wardriving-tekniikalla. Tätä tekniikkaa käytetään yleisemmin Wi-Fi-verkkojen datan keräämiseen. Tässä tutkimuksessa keskitytään kuitenkin yksinomaan muihin tiedonsiirtoteknologioihin, sillä Wi-Fi-verkkojen Wardrivingia on jo toteutettu laajasti Kotkansaarella (Fortinet s.a.; WiGLe.net 2024).

Tyypillisiä työkaluja ovat radiovastaanottimet, GPS-paikantimet sekä erilaiset ohjelmistot, jotka on suunniteltu käsiteltävän datan tallentamista ja analysointia varten. Vaikka wardrivingia voidaan käyttää tietoturva-aukkojen tunnistamiseen ja korjaamiseen, sitä voidaan myös väärinkäyttää hyökkäysten suunnittelussa ja toteuttamisessa (What is Wardriving? s.a.).

3.2 Bluetooth ja Bluetooth Low Energy (BLE)

Bluetooth-teknologia on tiedonsiirtotekniikka, jolla on merkittävä asema nykyaikaisessa IoT-laitteiden tietoliikenteessä. Se mahdollistaa lyhyen matkan kommunikoinnin ja erityisesti likiverkon käytön, joka käyttää vain vähän energiaa viestinnän aikana (Learn About Bluetooth s.a.).

Näiden ominaisuuksien ansiosta Bluetooth-teknologia on integroitunut olennaiseksi osaksi useimpia esineiden internetin (IoT) laitteita. Tästä syystä tämä tutkimus keskittyy myös Bluetooth-signaalien tutkimiseen.

Bluetooth Low Energy on langaton viestintätekniikka, joka on suunniteltu erityisesti energiatehokkaaseen ja suhteellisen hitaisiin tiedonsiirtoyhteyksiin. Se on kehitetty parantamaan Bluetooth-standardin käyttöä, erityisesti pienissä rajoitetuissa laitteissa, kuten älypuhelimissa, älykelloissa ja erilaisissa antureissa. BLE mahdollistaa laitteiden välisen lyhyen etäisyyden kommunikoinnin (Learn About Bluetooth s.a.).

BLE:n kehitysversio 4.0 on keskittynyt parantamaan Bluetooth-tekniikan tehokkuutta, turvallisuutta ja ominaisuuksia. BLE:n perusperiaate on pitää energiankulutus mahdollisimman alhaisena myös silloin, kun laitteet ovat aktiivisessa kommunikaatiossa (Decuir 2010).

Yksi BLE:n hyödyntäjistä ovat IoT-laitteet. Kommunikaatio IoT-laitteiden välillä vaatii usein pientä tiedonsiirtonopeutta ja pitkää akunkestoa, jotka ovat BLE:n vahvuuksia (Fürst ym. 2018). Esimerkiksi kotiautomaatiosovelluksissa BLE-teknologiaa käytetään erilaisten antureiden, kuten liiketunnistimien ja lämpötila-antureiden, hallintaan ja tiedonsiirtoon (Soumyalatha ym. 2016).

BLE:ssä on myös ominaisuuksia, jotka parantavat tietoturvaa, kuten salaus ja oikeanlainen yhteydenhallinta (Georgakakis ym. 2011). Tämä on tärkeää erityisesti terveydenhuollon kaltaisissa sovelluksissa, joissa tietoturva on ensisijaisen tärkeää.

Bluetooth Low Energy on siis langaton viestintätekniikka, joka on suunniteltu pienille, virtaa rajoitetuille laitteille, tarjoten energiatehokkaan ja turvallisen tavan siirtää tietoa lyhyillä etäisyyksillä (Learn About Bluetooth. s.a.).

3.3 Software-defined Radio (SDR)

Software-defined Radio (SDR) tarkoittaa radiota, josta on korvattu analoginen prosessointi digitaalisen prosessoinnin avulla. Näissä radioissa analogiset radiosignaalit muunnetaan digitaaliseen muotoon ja signaali käsitellään tietokoneella ajettavalla ohjelmistolla. Ohjelmisto käsittelee tarvittavat modulaatiot, demodulaatiot, suodattamisen ja muut tarpeelliset käsittelyt. (About RTL-SDR s.a.).

Suurin hyöty SDR-radioiden käytössä esimerkiksi tässä tutkimuksessa on niiden joustavuus ja tässä tapauksessa vielä itse laitteen halpa hinta, joka voi tukea tutkimuksen jatkokehitystä.

3.4 Industrial, Scientific and Medical (ISM)

Ohjelmistoradio-teknologiaa käytetään tässä tutkimuksessa ISM-taajuksilla toimivien protokollien vastaanottamiseen. ISM-taajuudet, eli Industrial,

Scientific and Medical -taajuudet, ovat taajuusalueita, jotka on varattu teollisuuden, tieteen ja lääketieteen käyttöön. Näillä taajuuksilla langattomat laitteet voivat toimia ilman erillisiä lisenssejä, mikä mahdollistaa laajan ja monipuolisen käytön eri IoT-laitteissa. Myös aikaisemmin mainittu Bluetooth-teknologia toimii näillä taajuuksilla, eli Bluetoothin tapauksessa 2.4 Ghz:n taajuusalueella. (Radiotaajuusmääräys 4AE2024M; Learn About Bluetooth. s.a.).

Näistä ISM-taajuuksista ehkä yleisimmin käytetyt taajuudet ovat 433.92 MHz ja 2.4 GHz. Tämä arvio perustuu siihen, että lähes kaikki yksinkertaiset lyhyen kantaman radiotaajuuksia käyttävät 433.92 MHz:n keskitaajuutta. Tämän voi havaita käytännössä tutkimalla esimerkiksi oman kodin IoT-laitteita, sekä vaikka langatonta auton avainta. Jälkimmäistä taajuusaluetta käyttävät taas Bluetooth- ja Wi-Fi-laitteet, joita tiedetään yleisesti olevan valtava määrä.

Syy kyseisten taajuuksien laajaan käyttöön löytyy todennäköisesti taajuuksien teknisistä ominaisuuksista, kuten kantoaallon taajuudesta ja kaistanleveydestä. Esimerkiksi 433.92 MHz sijoittuu matalan taajuuden alueelle (Radiotaajuusmääräys 4AE2024M). Tämä tarkoittaa sitä, että se tarjoaa pidemmän kantaman ja paremman läpäisevyyden esteiden läpi verrattuna korkeamman taajuuden alueisiin. Taajuuden 433.92 MHz kaistanleveys on tyypillisesti rajallisempi kuin korkeammilla taajuusalueilla (Radiotaajuusmääräys 4AE2024M). Tämä rajoittaa fysiikan lakien vuoksi tiedonsiirtonopeutta ja datan määrää, joka voidaan välittää yhdellä kerralla.

Taajuus 2.4 GHz on korkeampi kuin esimerkiksi 433.92 MHz. Tämä tarjoaa suuremman tiedonsiirtonopeuden ja enemmän kaistanleveyttä. Kyseinen taajuusalue tarjoaa kuitenkin lyhyemmän kantaman sekä huonomman läpäisevyyden esteiden läpi verrattuna matalampiin taajuusalueisiin. Leveämpi kaistanleveys ja suurempi tiedonsiirtonopeus vaikuttavat kuitenkin olevan ratkaisivia tekijöitä Bluetooth- ja Wi-Fi-laitteiden osalta.

3.5 Internet of Things (IoT)

Termi esineiden internet (IoT) viittaa fyysisten laitteiden, kuten antureiden, aktuaattorien ja muiden esineiden kykyyn kerätä, välittää ja vastaanottaa

tietoa digitaalisen viestinnän avulla. IoT-laitteet ovat monipuolisia, sillä ne voidaan implementoida lähes mihin vain laitteeseen (Madakam ym. 2015).

IoT-laitteiden ominaisuudet vaihtelevat suuresti niiden käyttötarkoituksen mukaan. Esimerkiksi älykkäissä kodinkoneissa ne mahdollistavat etäohjauksen ja reaaliaikaisen seurannan, kun taas teollisuuden IoT-laitteet voivat tuoda tehtaisiin tehokkuutta ja ennakoivaa ylläpitoa (Soumyalatha ym. 2016).

Käytännössä IoT-laitteet luovat fyysisten laitteiden ja järjestelmien ekosysteemin, jotka kommunikoivat keskenään ja keräävät sekä jakavat dataa. Tämä tapahtuu useimmiten ilman ihmisten suoraa vaikutusta. Tämä luo uusia mahdollisuuksia älykkäille sovelluksille, mutta samalla se asettaa haasteita tietoturvalle (Soumyalatha ym. 2016).

Koska monet IoT-laitteet toimivat langattomissa verkoissa, niiden tietoturva voi olla altis erilaisille hyökkäyksille, kuten etäohjaukselle, datan väärinkäytölle ja palvelunestohyökkäyksille (Lee 2020).

3.6 Wardriving-laitteisto

Pakettien vastaanottamiseen käytetään neljää RTL-SDR-radiovastaanotinta ja yhtä Bluetooth-vastaanotinta. RTL-SDR-radiovastaanottimet toimivat laajalla radiospektrumilla ja siksi ne sopivat myös yleisimpien ISM-taajuuksien vastaanottoon. Laite sisältää Realtek RTL2832U-mikropiirin, joka on alun perin kehitetty TV-signaalien vastaanottamiseen. Laitteesta on myöhemmin kehitetty yhteensopiva erilaisten ajureiden ja ohjelmistojen kanssa, jotka mahdollistavat laitteen käytön ohjelmistoon perustuvana radiovastaanottimena (eng. Software-Defined Radio) (About RTL-SDR. s.a.; Osmocom 2016).

Bluetooth-vastaanottimena käytetään geneeristä Bluetooth-vastaanotinta, joka kykenee vastaanottamaan aikaisemmin mainittuja lyhyenmatkan langattoman likiverkon mainostuspaketteja. Kyseessä voi olla esimerkiksi sisäänrakennettu Bluetooth-adapteri, joka on valmiiksi käytössä joissakin tutkimuksessa käytettävässä laitteessa.

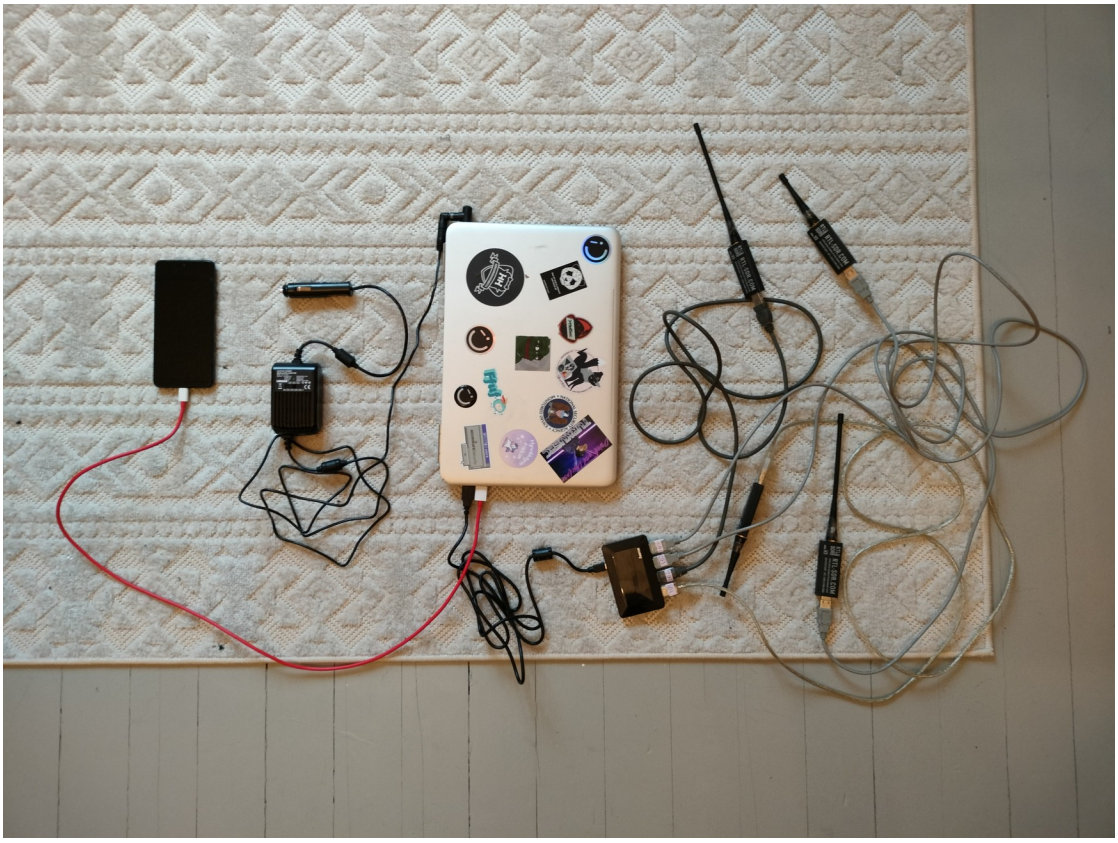
Laitteisto koostuu kokonaisuudessaan kannettavasta tietokoneesta, neljästä RTL-SDR-laitteesta, Android-puhelimesta ja Bluetooth-vastaanottimesta. RTL-SDR-laitteissa on antennit, jotka ovat tarkoitettu tutkittaville taajuuksille (433 MHz ja 868 MHz). Muille tutkimuksessa käytettäville taajuuksille (315 MHz ja 915 MHz) käytetään samoja antenneja (433 MHz ja 868 MHz), sillä juuri näille taajuuksille ei ollut saatavilla täysin oikeanlaisia antenneja. Antennien taajuusalueet ovat kuitenkin suhteellisen lähellä toisiaan, joten niillä voi olla mahdollista vastaanottaa myös näitä taajuuksia. Tämä toimintatapa otetaan kuitenkin huomioon lopputulosten arvioinnissa.

Lisäksi antennien sijoitus henkilöautossa toteutetaan siten, että radiosignaalien ja vastaanottimien välissä on mahdollisimman vähän esteitä. Auton metallinen kori voi esimerkiksi vaikuttaa negatiivisesti vastaanottokykyyn (Zuazola ym. 2012).

Tutkimuksessa käytettävän kannettavan tietokoneen akun kestävyydestä ei ole tarkkaa tietoa. Tästä syystä tutkimuksen onnistumisen varmistamiseksi kannettavan tietokoneen lataamiseen käytetään laturia, jota voidaan käyttää henkilöautossa. Tällä tavoin varmistetaan tietokoneen jatkuva virransaanti. Tietokoneen oma sisäinen akku varmistaa tutkimusdatan keräämisen, vaikka virran saaminen keskeytyisi hetkeksi, esimerkiksi auton sammumisen johdosta.

RTL-SDR-laitteet ovat yhdistettyinä USB-jatkokaapeleilla USB-hubiin. Tämä mahdollistaa antennien asettamisen esimerkiksi henkilöauton kojelaudalle. Bluetooth-vastaanottimena voidaan käyttää puhelimen sisäistä, kannettavan tietokoneen sisäistä tai ulkoista Bluetooth-sovitinta, joka liitetään kannettavaan tietokoneeseen USB-portin kautta. Tässä tutkimuksessa pakettien vastaanottamiseen käytetään helposti saatavia ja halpoja radiovastaanottimia. Tällä tavoin tutkimuksen tuloksia voidaan pitää realistisina kyberuhkina, joita kuka vain tarpeeksi asiasta tietävä voisi toteuttaa. Tämä laajentaa mahdollisuuksia yhdistää havaittavia kyberuhkia konkreettisiin elämäntilanteisiin, tuoden lisäarvoa tutkimuksen tuloksille. Wardrivingissa oleellinen GPS-seuranta toteutetaan Android-puhelimen GPS-moduulia hyödyntäen, sillä puhelin on mahdollista yhdistää Kismet-ohjelmistoon (Daveking Wiki 2021).

Kokonaisuudessaan laitteisto koostuu laitteista, joiden käyttötarkoitukset on määritelty tarkasti, ja niiden yhteensopivuus on varmistettu testaamalla niiden toimivuus käytännössä (kuva 2). Tämä testaus on suoritettu ennen varsinaisen Wardrivingin aloittamista.



Kuva 2. Kuvassa GPS-vastaanotin (Android-puhelin), autolaturi kannettavalle tietokoneelle, kannettava tietokone, USB-hubi ja neljä RTL-SDR-vastaanotinta

3.7 Wardriving-ohjelmisto

Tässä tutkimuksessa käytetään ohjelmistoa nimeltään ”Kismet”, joka perustuu avoimeen lähdekoodiin. Avoimen lähdekoodin ohjelmiston käyttö tutkimuksen toteutuksessa tarjoaa monia etuja. Avoimen lähdekoodin ohjelmistot ovat yleensä ilmaisia käyttää. Tämä on hyödyllistä tutkimukselle, jolla ei ole käytettävissä suurta budjettia. Lisäksi avoimen lähdekoodin ohjelmistot ovat yleensä mukautettavissa erilaisiin tarpeisiin, mikä mahdollistaa tarvittavien muokkausten tekemisen (AlMarzouq ym. 2005).

Avoimen lähdekoodin ohjelmistoilla on usein aktiivinen kehittäjäyhteisö, joka tarjoaa apua ja tukea. Avoimen lähdekoodin ohjelmistojen käyttö mahdollistaa myös helpon jatkokehityksen tutkimukselle, sillä ohjelmistolla on yleensä hyvä

saatavuus. Lisäksi osa tutkijoista saattaa arvostaa avoimen lähdekoodin periaatteita ja pyrkii aktiivisesti tukemaan niitä valitsemalla avoimen lähdekoodin ohjelmistoja (AlMarzouq ym. 2005). Tämä valinta perustuu eettisiin ja filosofisiin näkökohtiin sekä teknisiin seikkoihin, kuten resurssien saatavuuteen ja teknologian näkökulmasta jatkotutkimuksen helpottamiseen.

Kismet tarjoaa kätevän työkalun langattomien verkkoympäristöjen analysointiin ja seurantaan. Kismet mahdollistaa muun muassa RF- ja Bluetooth-laitteiden tunnistamisen yhdessä RTL_433-ohjelmiston kanssa (Kismet s.a.). RTL_433-ohjelmisto on erillinen avoimen lähdekoodin ohjelmisto, jota käytetään ISM-taajuuksia käyttävien laitteiden tutkimiseen (Github s.a.).

Kismetin avulla voidaan siis havaita, tunnistaa ja analysoida useita eri protokollia käyttäviä IoT-laitteita. Lisäksi Kismet osaa yhdistää havaitut laitteet GPS-dataan ja tällä tavoin Kismetin keräämän datan avulla voidaan luoda esimerkiksi karttoja, joista käy ilmi löydettyjen laitteiden sijainnit (Kismet s.a.).

3.8 Tulosten analysointi

Tulokset ovat tässä tutkimuksessa dataa, joka on kerätty radiorajapinnasta. Löydöksenä voidaan olettaa löytyvän ainakin joitakin IoT-laitteita ja jotkut löydetyistä laitteista saattavat olla haavoittuvaisia joillekkin hyökkäyksille.

Tutkimuksessa käytettävä data tallennetaan luotettavalle alustalle, kuten yleisesti vakaana pidetylle Linux-jakelulle. Tämä saattaa parantaa datan turvallista säilytystä ja edistää tutkimuksen sujuvaa toteutusta. Lisäksi tutkimuksessa käytettävät ohjelmistot tukevat laajasti Linuxiin perustuvia jakeluita.

Tapaustutkimuksen menetelmiä hyödyntäen tulokset on määrä saada esitettäväksi selkeään muotoon ja niin, että tutkimuksesta voidaan vetää johtopäätöksiä Kotkansaaren IoT-laitteiden kyberturvallisuuden tilasta. Aineisto kerätään siihen soveltuvalla avoimen lähdekoodin ohjelmistolla.

Tällä menetelmällä saadut tulokset visualisoidaan esimerkiksi LibreOfficen taulukkolaskentaohjelmalla. Datan analysoinnissa käytetään yksinkertaista kuvailevaa tilastollista analyysiä. Tämä sisältää peruslaskelmia, jotka perustuvat todennäköisesti kolmeen eri pääasialliseen muuttujaan; aika, paikka ja laitetyyppi. Yksinkertainen analyysi sopii hyvin Wardriving-tutkimukseen. Tämä johtuu siitä, että yksinkertainen analyysi voi auttaa hahmottamaan havaittuja ilmiöitä ilman liiallista monimutkaisuutta (Lähdesmäki ym. 2009).

Tulokset visualisoidaan lopuksi myös kartalla, sillä karttojen käyttö antaa selkeän käsityksen siitä, missä päin aluetta tiettyjä IoT-laitteita löytyy tai missä paikoissa on havaittavissa tietoturva-aukkoja. Karttaohjelmana käytetään Google Earth Prota, sillä sen ominaisuudet tukevat tutkimuksen toteuttamista.

Saatuja tuloksia tulkitaan vertaamalla niitä sekundääriaineistoon. Tämän perusteella voidaan myöhemmin selvittää mahdollisten haavoittuvuuksien vakavuutta, yleisyyttä ja vaikutusta reaalimaailman skenaarioihin. Lisäksi tutkimustulosten perusteella pohditaan, miten tulokset vastaavat alkuperäisiin tutkimuskysymyksiin ja tavoitteisiin.

Vaikka mahdolliset rajoitukset ja tutkimuksen vahvuudet voidaan osittain päätellä ennakkoon, on hyvä tunnistaa, että sekundääriaineiston mahdollinen puutteellisuus saattaa vaikeuttaa näiden arviointia etukäteen. Lisäksi tulosten julkisuutta rajoittavat eettiset näkökohdat, kuten se, mitkä tiedot voidaan julkaista ilman haitallisia vaikutuksia yleiseen turvallisuuteen. Näitä ovat esimerkiksi yksityiset henkilö- ja yritystiedot, paikkatiedot, käyttötiedot, dataliikenteen tiedot, sensoreiden keräämät tiedot, sekä käyttäytymistiedot (Pseudonymisoidut ja anonymisoidut tiedot. s.a.).

Tulokset anonymisoidaan asianmukaisilla tietosuojatoimenpiteillä, jotka noudattavat asianmukaisia säädöksiä ja standardeja, jotta käyttäjien yksityisyys ja tietoturva säilyvät. Nämä toimenpiteet pyrkivät säilyttämään tutkimuksen luotettavuuden ja sen yhteyden reaalimaailman skenaarioihin, samalla kun ne estävät tuloksia osoittamasta esimerkiksi yksittäisten yritysten tietoturvan tasoa (Mikä on henkilötieto? s.a.). Tämä toteutetaan käytännössä

niin, että tutkimustuloksista poistetaan tutkimuksen onnistumisen kannalta tarpeettomat yksilöllistävät tiedot.

Tutkimuksessa keskitytään dataan, joka on kerättävissä vapaasti. Tämä tarkoittaa sitä, että tutkittaviin laitteisiin ei olla yhteydessä millään tavoin. Kaikki mahdollinen data saadaan pelkästään vastaanottamalla passiivisesti laitteiden lähettämiä datapaketteja.

Kyseiset paketit ovat esimerkiksi aikaisemmin mainittuja Bluetooth-teknologian LE-Advertisement -datapaketteja, eli lyhyenmatkan langattoman lähiverkon mainostuspaketteja tai yleisimmillä ISM-radiotaajuuksilla toimivia paketteja, jotka voivat vaihdella sisällöltään paljonkin (Kail ym. 2018; Fürst ym. 2018).

Mahdollisen jatkokehityksen kannalta voisi olla hyödyllistä laajentaa tutkimusta lisäämällä erilaisia datalähteitä ja analyysimenetelmiä. Yksityiskohtaisempi tutkimus voisi keskittyä syvemmin erilaisten laitteiden haavoittuvuuksiin ja niiden esiintymiseen eri paikoissa. Lisäksi voitaisiin tarkastella ajan ja paikan vuorovaikutusta haavoittuvuuksien ilmenemisessä.

Tämä voisi sisältää esimerkiksi aikasarja-analyysiä sekä alueellisten erojen tutkimista haavoittuvuuksien esiintymisessä. Tällaiset laajennetut analyysit voisivat tarjota syvällisempää ymmärrystä IoT-laitteiden tietoturvatilanteesta ja auttaa suunnittelemaan tehokkaampia turvatoimia Kotkansaarella ja vastaavilla alueilla. Laajemmat analyysit vaativat enemmän aikaa datan keräämisessä, joten tässä tutkimuksessa käsitellään aihealuetta vain pintapuolisesti.

Valmiiksi rakennetun laitteiston tarjoama pohja voi olla hyödyllinen lähtökohta uusien ominaisuuksien ja parannusten kehittämisessä. Kyseinen laitteisto on helposti saatavilla ja kohtuuhintaista, mikä tekee siitä joustavan ja soveltuvan erilaisiin käyttötarkoituksiin. Tämä helpottaa jatkokehitystä ja mahdollistaa tutkimuksen tehokkaan hyödyntämisen. Lisäksi tutkimuksen antama esimerkki Wardriving-ohjelmiston käytöstä voi helpottaa jatkokehityksen toteuttamista.

3.9 Lailliset käytännöt ja eettinen harkinta

Wardriving on datan keruumuoto, joka herättää sekä eettisiä että laillisia kysymyksiä. Wardriving on laillista suuressa osassa maailmaa ja Suomenkaan radiolaissa ei näytä olevan erityistä kieltoa Wardrivingiin liittyvien toimintojen, kuten radiosignaalien vastaanottamisen, osalta (Fortinet s.a.; Radiolaki 16.11.2001/1015). Myös muun sekundääriaineiston pohjalta voidaan todeta, että tutkimuksen suorittamiselle ei näytä olevan laillisia esteitä.

Tutkimuksen etiikka on tärkeä osa hyvää tieteellistä tutkimusta ja tarve eettiselle pohdinnalle korostuu erityisesti silloin kun käsitellään tietoturvaa ja yksityisyyttä koskevia kysymyksiä. Tutkimuksen tuloksista saattaa esimerkiksi paljastua tietoja, joista voi olla haittaa tietoturvalle ja yksityisyydelle. Tutkimuksessa on siksi harkittava, miten kerättyä tietoa käytetään ja jaetaan sekä miten yksityisyyttä suojataan. Tästä syystä tutkimuksen tuloksissa ei esimerkiksi paljasteta yksityisiä tietoja, jotka eivät ole relevantteja tutkimuksen onnistumisen kannalta.

Tutkimuksen tulokset on myös esitettävä objektiivisesti ja totuudenmukaisesti. Tämä on tutkimuksen luotettavuuden kannalta välttämätöntä. Siksi tutkimuksessa käytetyt menetelmät ja tarkoitukset ovat läpinäkyviä ja niitä voidaan tarvittaessa toistaa.

Lisäksi on punnittava tutkimuksen tuomia hyötyjä ja haittoja. Julkinen tieto esimerkiksi haavoittuvuuksista kriittisessä infrastruktuurissa voi aiheuttaa riskejä yleiselle turvallisuudelle.

Toisaalta haavoittuvuuksien pysyminen salassa aiheuttaa vielä sitäkin suurempia riskejä, sillä ongelmia ei voida korjata ennen kuin niistä ollaan tietoisia. Julkisella ilmoittamisella mahdollistetaan haavoittuvuuksien paikkaaminen ennen niiden hyväksikäyttöä mahdollisen hyökkääjän toimesta.

Julkinen ilmoittaminen haavoittuvuuksista voi myös painostaa käyttäjiä korjaamaan tietoturvaongelmia. On yleistä, että käyttäjille kerrotaan haavoittuvuudesta, mutta he eivät kuitenkaan ryhdy tarvittaviin toimenpiteisiin

suojatakseen itseään. Vasta kun haavoittuvuudet tulevat julkisiksi, tapahtuu yleensä muutoksia. Ehkä siksi, että uhka näyttää todennäköisemmältä ja vakavammalta.

Eettisyyden yhteenvetona voidaan siis todeta, että tutkimuksessa on tärkeää huolehtia eettisistä tutkimustavoista, jotta voidaan minimoida tutkimustulosten mahdolliset haitat ja samalla maksimoida niistä saatavat hyödyt.

4 TUTKIMUKSEN TOTEUTUS

4.1 Laitteisto ja ohjelmisto

Tutkimus aloitettiin tutkimalla ohjelmistopuolen mahdollisuuksia. Sekundääriaineiston pohjalta huomattiin, että Kismet-ohjelmiston avulla voidaan suorittaa Bluetooth- ja radiosignaalien Wardrivingia (Kismet s.a.). Kismet osaa myös hyödyntää lähteenä Rtl_433-ohjelmistoa, joka helpottaa merkittävästi Wardrivingin toteuttamista. Lisäksi Kismet-ohjelmistoon voidaan yhdistää Android-puhelin, jolloin sitä voidaan käyttää GPS-seurannan lähteenä. Näiden ominaisuuksien, sekä muiden teknisten seikkojen vuoksi Wardriving-ohjelmistoksi valittiin Kismet.

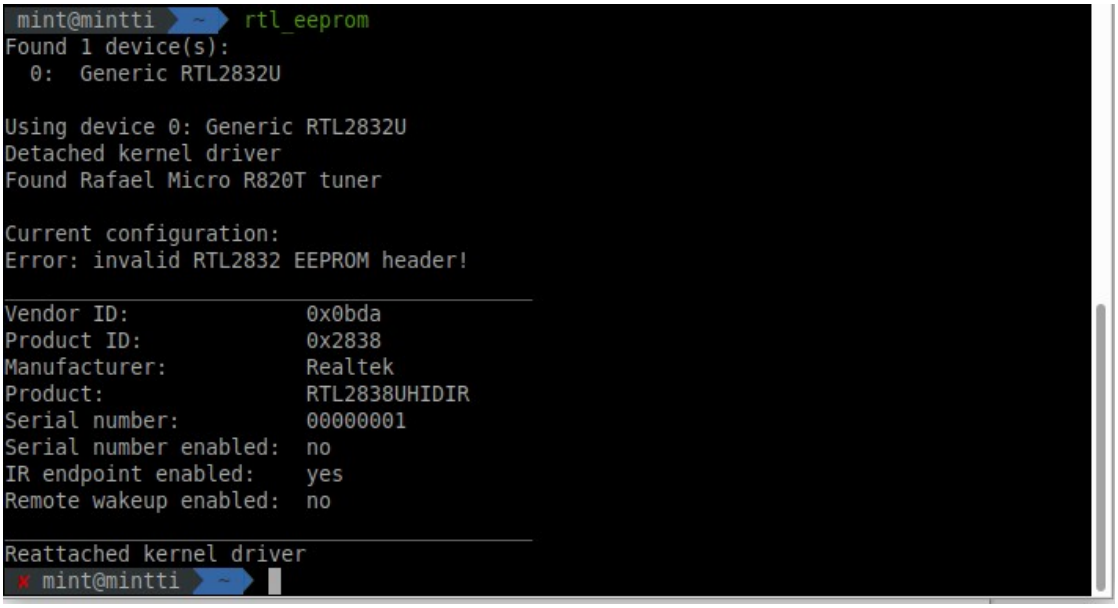
Seuraavaksi pohdittiin laitteistopuolta, sekä sitä miten ohjelmisto ja laitteisto yhdistetään toimivaksi kokonaisuudeksi. Laitteiston on määrä olla sellaista, että se tukee mahdollisimman hyvin ohjelmiston tarjoamia mahdollisuuksia. Käytännössä tämä tarkoittaa sitä, että edellä mainitut Kismetin tarjoamat toiminnot saadaan ylipäätään toteutettua.

Alkuperäisen suunnitelman mukaan RTL-SDR-radiovastaanottimia on vain kaksi kappaletta, joiden avulla on määrä saada tietoa taajuuksista 433.92 MHz ja 868 MHz. Tutkimalla sekundääriaineistoa uudestaan huomattiin kuitenkin, että radiovastaanottimia voidaan lisätä Kismettiin ilman sen kummempia järjestelyitä. Tästä syystä laitteistoon lisättiin vielä kaksi radiovastaanotinta. Tämä toi mahdollisuuden saada tutkimusdataa myös taajuuksista 315 MHz ja 915 MHz. Taajuudet valittiin siksi, että ne kuuluvat IoT-laitteiden käyttämiin taajuusalueisiin, kuten edellä mainitut 433.92 MHz ja 868 MHz (Github. s.a.). Bluetooth-vastaanottimena käytettiin kannettavan tietokoneen sisäistä vastaanotinta, kuten oli aiemmin suunniteltu.

Laitteistoa tuli siis suhteellisen paljon yhdelle kannettavalle tietokoneelle. Ongelmaksi tulikin se, että tietokoneessa on vain kaksi toimivaa USB-liitäntää ja liitettäviä laitteita oli enemmän. Ratkaisuna lisättiin nelipaikkainen USB-hubi. Radiovastaanottimien toimivuus kokeiltiin Rtl_test-ohjelmistolla, jolla voidaan testata laitteiden toimivuutta (kuva 3) (Debian käyttöohjeet. s.a.).

Kuva 3. Kuvassa testataan yhden radiovastaanottimen toimivuutta Rtl_test-ohjelmiston avulla

Tuloksena ilmeni, että laitteet eivät toimineet ollenkaan, kun ne olivat liitettyinä USB-hubiin. Syyksi epäiltiin ensimmäiseksi sitä, että kaikilla vastaanottimilla oli sama sarjanumero: ”00000001”. Tämä voisi aiheuttaa ongelman, jossa ohjelmisto olettaa kaikkien laitteiden olevan yksi ja sama laite, joka johtaa siihen, että ohjelmisto ei toimi määrätyllä tavalla. Tästä syystä laitteiden sarjanumerot vaihdettiin niin, että jokaisella niistä on yksilöllinen numero. Ohjelmistona tähän käytettiin rtl_eepromia (kuva 4).



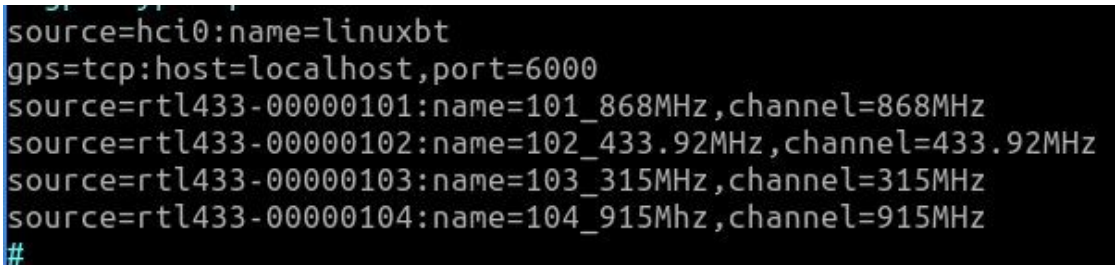
Kuva 4. Kuvakaappaus rtl_eepromin käytöstä

Sarjanumeroiden vaihtaminen ei kuitenkaan tuottanut haluttua tulosta, joten alettiin pohtimaan sitä, käyttävätkö radiovastaanottimet yksinkertaisesti liikaa virtaa tai viekö niiden käyttämä data liikaa kaistanleveyttä. Ongelman selvittämisen helpottamiseksi päätettiin kuitenkin, että kokeillaan toista USB-hubia. Päätös tehtiin siksi, että voi olla helpompaa kokeilla uutta laitetta ennen kuin lähdetään etsimään lisää sekundääriaineistoa radiovastaanottimien teknisten vaatimusten osalta. Uuden USB-hubin käyttöönotto ratkaisikin ongelman heti, eikä ongelman ratkaisuun tarvittu esimerkiksi USB-hubia, jossa olisi ollut ulkoinen virtalähde. Ongelma ei siis johtunut aikaisemmin spekuloiduista seikoista. Aikaisemmin käytetty USB-hubi ei vain jostain tuntemattomaksi jääneestä syystä toiminut muun laitteiston kanssa.

GPS-laitteisto, eli Android-puhelin toteutettiin niin, että puhelimelle ladattiin F-droid-sovelluskaupasta sovellus nimeltä: ”gpsdRelay”. Kyseisellä sovelluksella voidaan välittää puhelimen vastaanottamaa GPS-signaalia eteenpäin TCP- tai UDP-protokollan avulla. Tämä tarkoitta sitä, että GPS-data voidaan kuljettaa verkkoliikenteen välityksellä. Erillisen Wi-Fi-tukiaseman luominen olisi mahdollistanut puhelimen yhdistämisen kannettavaan tietokoneeseen ilman USB-liitännän käyttöä. Lopulta kuitenkin päädyttiin siihen, että ADB:n (eng. Android Debug Bridge) avulla ohjatiin gpsdRelayn käyttämä portti kannettavan tietokoneen paikallisosoitteeseen (eng. Localhost) käyttäen hyödyksi USB-liitäntää. Tämä toimintatapa poisti tarpeen erilliselle Wi-Fi-tukiasemalle, joka

olisi lisännyt sekä laitteiston monimutkaisuutta että riskiä ongelmille. Adb:n käyttö edellyttää kehittäjäasetusten sallimista Android-puhelimessa.

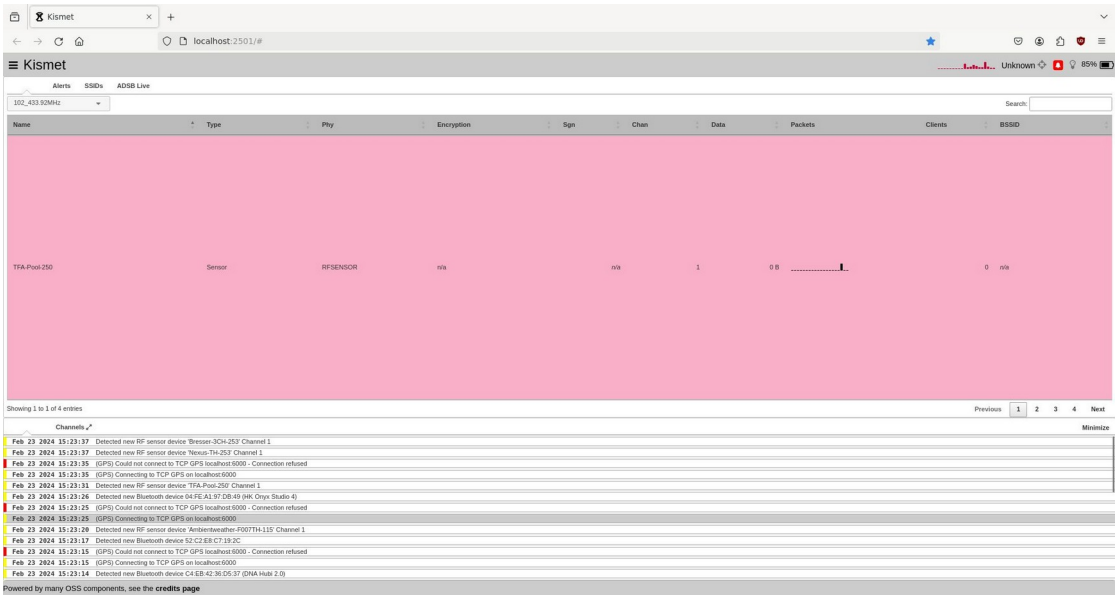
Tähän asti koottu yhdistelmä laitteistosta ja ohjelmistosta testattiin, jotta voitiin todeta mahdolliset ongelmat ennen varsinaista Wardrivingin suorittamista. Testaaminen aloitettiin valmistelemalla Kismetin konfiguraatiotiedosto (kismet.conf) sellaiseksi, että Kismet käyttää jokaista laitetta ja oikealla tavalla (kuva 5).



Kuva 5. Näyttökaappaus Kismetin konfiguraatiotiedostosta

Ensimmäiseksi asetettiin Bluetooth-laitteeksi kannettavan sisäinen Bluetooth-adapteri. Sitten määriteltiin GPS-laitteen tyyppi, osoite ja portti. Tämän jälkeen määriteltiin kaikki Rtl_433-ohjelmiston lähteet eli radiovastaanottimet. Jokainen vastaanotin lajiteltiin sarjanumeroiden mukaan ja kaikille niistä annettiin oma vastaanottotaajuus. Tämän jälkeen tietokoneelta käskettiin Android-puhelinta luomaan porttien 6000 välinen yhteys komennolla: ”adb forward tcp:6000 tcp:6000”. Tällä tavoin mahdollistetaan GPS-tietojen siirtäminen puhelimelta tietokoneelle ja lopulta Kismet-ohjelmistolle. Tietokoneelta laitettiin lisäksi päälle GPS-daemon komennolla: ”gpsd -N -n -D5 tcp://localhost:6000” jotta gpsd voi vastaanottaa GPS-dataa TCP-yhteyden kautta paikallisesta portista 6000.

Seuraavaksi käynnistettiin Kismet komennolla: ”kismet”. Kismetin antaman tiedon mukaan yhteys GPS:ään ja muihin laitteisiin onnistui. Tämän jälkeen avattiin Kismetin käyttöliittymä menemällä selaimella osoitteeseen: ”localhost:2501”. Käyttöliittymässä näkyy perustietoja esimerkiksi löydetyistä IoT-laitteista (kuva 6).



Kuva 6. Näyttökaappaus Kismetin graafisesta käyttöliittymästä

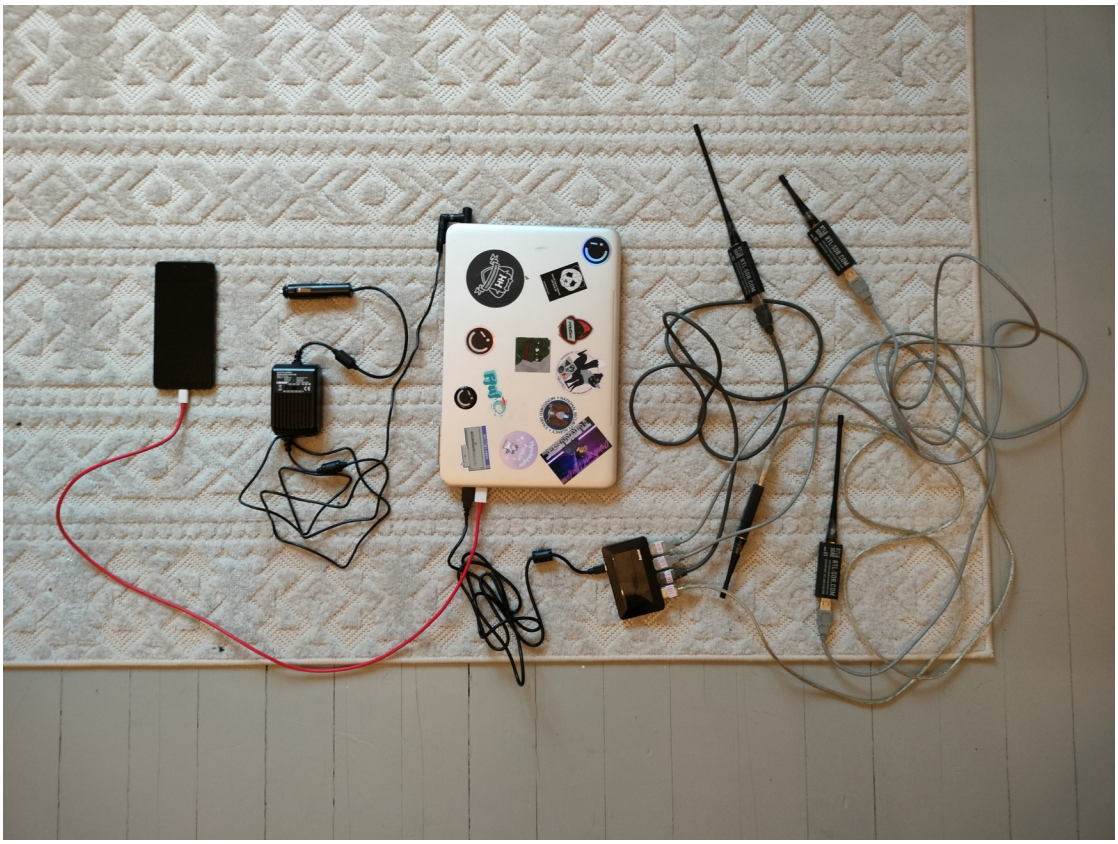
Edellä mainittu kuva on vain esimerkkikuva ja yksityisyyden takia GPS-laitetta ei ole vielä yhdistetty. GPS-laitteen antamat koordinaatit näkyisivät kuitenkin oikeassa yläkulmassa tekstin: ”Unknown” -tilalla, jolloin voidaan todeta GPS:n toimivuus.

Laitteiston ja ohjelmiston toimivuus todettiin keräämällä tarpeeksi dataa niin, että voitiin nähdä eri vastaanottimien kaappaavan tietoja onnistuneesti ympärillä olevista IoT-laitteista. Tämä onnistui suunnitelmien mukaan, mutta samalla ilmeni uusi ongelma. Kannettavan tietokoneen akku tyhjeni alle tunnissa, kun kaikki laitteet olivat yhdistettyinä tietokoneeseen. Tämä olisi ongelma, sillä Wardrivingin suorittamiseen saattaisi mennä enemmän aikaa kuin mitä akku kestää. Ongelma saatiin kuitenkin ratkaistua sillä, että kannettavalle hankittiin laturi, joka mahdollisti sen lataamisen autossa (kuva 7).

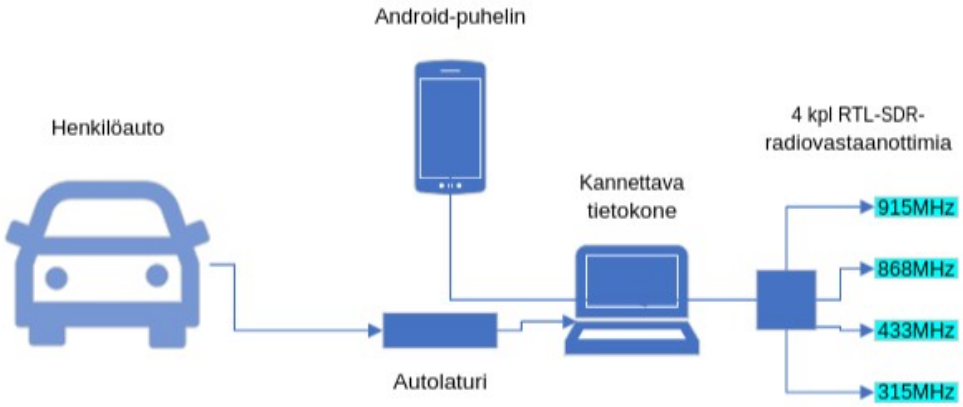
Kuva 7. Kuva laturista, joka mahdollistaa kannettavan lataamisen autossa

Tällä testaamisella saatiin lopulta toimiva ohjelmiston ja laitteiston muodostama kokonaisuus, jota voidaan testien perusteella käyttää Wardrivingin suorittamiseen. Laitteistokuva esitellään uudestaan, jotta sitä ja myöhempää kuvakaaviokuvaa voidaan vertailla helposti vierekkäin. Kuvassa (kuva 8) (alkaen vas.) Android-puhelin, sen vieressä autolaturi, kannettava tietokone, USB-hubi ja neljä RTL-SDR-radiovastaanotinta. Toisessa kuvassa (kuva 9) esitetään laitteisto vielä tarkemmin kuvakaavion avulla. Kuvasta

(kuva 9) käy ilmi myös radiovastaanottimien vastaanottotaajuudet, jotka ovat 915 MHz, 868 MHz, 433 MHz sekä 315 MHz.



Kuva 8. Kuva lopullisesta laitteistosta



Kuva 9. Kuvakaavio lopullisesta laitteistosta

4.2 Kohteiden määrittäminen ja reitin suunnittelu

Ennen Wardivingin suorittamista määritettiin reitti, jonka avulla oli määrä saada mahdollisimman paljon tutkimukselle hyödyllistä dataa. Ajettavan reitin

suunnittelu oli alun perin tarkoitus tehdä OpenStreetMapin avulla, mutta lopulta suunnittelu tehtiin Google Earth Pron avulla. Tämä johtui siitä, että Google Earth Pro tarjosi parempia ilmakuvia, mikä helpotti maastossa olevien kohteiden määrittämistä. Suunnitteluvaiheesa huomattiin myös, että erittäin tarkan reitin määrittäminen vaikuttaa huonolta idealta muun muassa siksi, että se vaatisi paljon aikaa ja resursseja, mikä puolestaan veisi aikaa muiden tutkimusaiheiden toteuttamiselta. Lisäksi tarkan reitin määrittäminen on haastavaa myös siksi, että liikennesäännöt, kuten yksisuuntaiset tiet, eivät välttämättä käy ilmi kartoista. Tämä johtaisi siihen, että reitti olisi suunniteltava uudelleen aina, kun sellaiseen törmätään Wardrivingin aikana.

Tästä syystä reitti päätettiin määritellä niin, että kartalle merkittiin tärkeimmät kohteet, joista voidaan arvella löytyvän mielenkiintoisia tuloksia. Tärkeimmät kohteet määriteltiin suurimmalta osin sen perusteella, että ne ovat alueita, joissa tiedetään olevan esimerkiksi teollisuutta tai muita alueita, joissa voisi olla paljon IoT-laitteita. Tärkeimmiksi kohteiksi merkittiin neljä eri kohdetta ilmakuvasta (kuva 10).

Kuva 10. Ilmakuva Kotkansaaresta, johon on merkitty tärkeimmät kohteet (Google 2022)

Tärkeimmät kohteet ovat seuraavat:

1. Lantmännen Ceralia Kotka ja Hankkija Oy Kotkan Rehutehdas
2. Kotkan merivartioasema ja FinFerries autolautta.
3. Kotkamills ja Kantasataman alue
4. Kotkan Sataman juna-asema ja Kotkan rautatieasema

Tärkeimpien kohteiden lisäksi suunniteltiin, että Kotkansaarta ajellaan ikään kuin satunnaisotannalla ja sen mukaan missä saattaisi olla eniten ihmisiä, eli esimerkiksi ydinkeskustassa ja joillakin asuinalueilla.

4.3 Ensimmäinen Wardriving

Wardriving suoritettiin kahdesti. Ensimmäinen Wardriving toteutettiin 21.2.2024 klo 13.30 alkaen. Vastaanottolaitteet sijoitettiin henkilöautoon niin, että auton metallinen kori estäisi radiosignaalien vastaanottamista mahdollisimman vähän (kuva 11).
Lisäksi tietokone asetettiin niin, että siitä pystyttiin huomaamaan mahdolliset Wardrivingin aikana tapahtuvat ongelmat, kuten esimerkiksi GPS-yhteyden katkeaminen (kuva 12). Tämä mahdollistaa Wardrivingin keskeyttämisen ja mahdollisten ongelmien korjaamisen. Aikaisemmin sunnitellun ohjelmiston lisäksi Android-puhelimeen ladattiin sovellus, jolla voitiin tallentaa henkilöautolla ajetun reitin sijaintidataa. Tämän ajateltiin olevan hyödyllistä myöhemmin, kun esitetään tutkimuksen tuloksia.

Kuva 11. Kuva RTL-SDR-radiovastaanottimista aseteltuna kojelaudan päälle

Kuva 12. Kuva Wardrivingin aikana käytetystä laitteistosta

Wardriving kesti n. 1,5 tuntia ja sen aikana onnistuttiin ajamaan läheltä kaikkia tärkeimpiä kohteita. Auton seuraamista varten asennettu GPS-seurantasovellus tallensi paikkatietodataa liian harvoin. Tästä syystä tallennettu reitti on hieman epätarkka (kuva 13). Kismet tallensi kuitenkin GPS-dataa tarkasti koko Wardrivingin ajan, joten tämän virheen ei pitäisi vaikuttaa merkittävästi tutkimuksen tuloksiin. Ajonopeus pyrittiin pitämään suurimmaksi osin 0–40km/h välillä, jotta radiovastaanottimet kerkeävät tallentamaan todennäköisemmin IoT-laitteiden lähettämiä datapaketteja. Tämä onnistui kaupunkialueella ajettaessa helposti, sillä myös muun liikenteen nopeus oli arviolta tätä luokkaa.

Kuva 13. Ilmakuva Kotkansaaresta ja ajettu reitti (Google 2022)

Kismetin tallentaman datan tarkastelun perusteella voitiin todeta, että Wardriving oli kokonaisuutta tarkastellen onnistunutta, sillä laitteita löytyi monilla eri vastaanottimilla. Lisäksi Kismet ei ilmoittanut virheistä, jotka vaikuttaisivat oleellisesti tutkimuksen onnistumiseen.

Datan tutkimisen aikana kävi ilmi, että Kismet oli jostain syystä tallentanut GPS-dataa pelkästään RF-laitteiden osalta. Syytä tälle selvitettiin ensimmäiseksi lukemalla Kismetin dokumentaatiota tarkemmin, mutta sen avulla ei löytynyt vastausta. Tämä jälkeen asiasta kysyttiin Kismetin Discord-kanavan teknisen tuen chatista. Aiheeseen vastasi yksi henkilö. Hän arvioi, että Kismetin idea on vain tallentaa Bluetooth-laitteista lista eikä merkitä niitä yhteen GPS-datan kanssa. Henkilö ohjasi käyttämään WiGLE:n sovellusta Androidilla, jolla voidaan toteuttaa Bluetooth-Wardrivingia.

Tutkimalla vielä lisää Kismetin tallentamaa dataa huomattiin kuitenkin, että Kismet tallensi periaatteessa GPS-koordinaatit yhdistettynä löydettyihin Bluetooth-laitteisiin, mutta tiedot on tallennettu tietueeseen. Tämä johtaa siihen, että esimerkiksi muuntamalla Kismetdb-tiedosto KML-tiedostoksi (eng. Keyhole Markup Language) voidaan havaita, että kartalla näkyvät ainoastaan RF-laitteet ja Kismet_to_kml sivuuttaa kokonaan Bluetooth-laitteet.

Tämän sekä datan oikeellisuuden vuoksi päätettiin suorittaa toinen Wardriving heti seuraavana päivänä. Toisen Wardriving yrityksen oli määrä korjata ensimmäisen Wardrivingin aikana havaittuja virheitä ja mahdollistaa se, että kahden eri kerran tuloksia voitaisiin vertailla keskenään.

4.4 Toinen Wardriving

Toinen Wardriving suoritettiin 22.2.2024 klo 21.30 alkaen. Lähtökohdat olivat muuten samanlaiset kuin ensimmäisellä Wardriving kerralla, mutta sen lisäksi ratkaistiin aikaisempia ongelmia. Tällä kertaa auton GPS-seurannassa käytetty sovellus asetettiin tallentamaan GPS-dataa mahdollisimman usein, jotta ajettua reittiä voitaisiin esittää kartalla tarkemmin. Lisäksi Bluetooth-Wardrivingin osalta käytettin WiGLE:n sovellusta Androidilla.

Ajettu reitti oli suurilta osin samanlainen kuin ensimmäisellä kerralla ja muutkin muuttujat, kuten Wardrivingin aikana käytetty nopeus olivat hyvin samalaisia. Reitti tallentui halutulla tavalla tarkemmin (kuva 14). Lisäksi WiGLE:n avulla löydettiin monta Bluetooth-laitetta, jotka tällä kertaa yhdistyivät kätevästi GPS-dataan.

Kuva 14. Ilmakuva Kotkansaaresta ja toisen Wardriving kerran reitti (Google 2022)

Kokonaisuudessaan voidaan katsoa, että Wardrivingin avulla on saatu tutkimuksen tavoitteiden osalta käyttökelpoista primääriaineistoa. Kerätystä datasta voidaan todennäköisesti tehdä päätelmiä turvallisuustilanteesta sekä arvioida eri IoT-laitteiden haavoittuvuuksia. Näitä tuloksia voidaan yhdistää sekundääriaineiston tietolähteisiin, mikä auttaa tuomaan esiin IoT-laitteiden turvallisuuskysymyksiä ja lisäämään tietoisuutta niiden mahdollisista riskeistä. Lisäksi nämä tulokset voivat tarjota tietoa, joiden avulla voidaan tehokkaasti suojata IoT-laitteiden käyttäjiä mahdollisilta uhilta.

5 TUTKIMUSTULOKSET

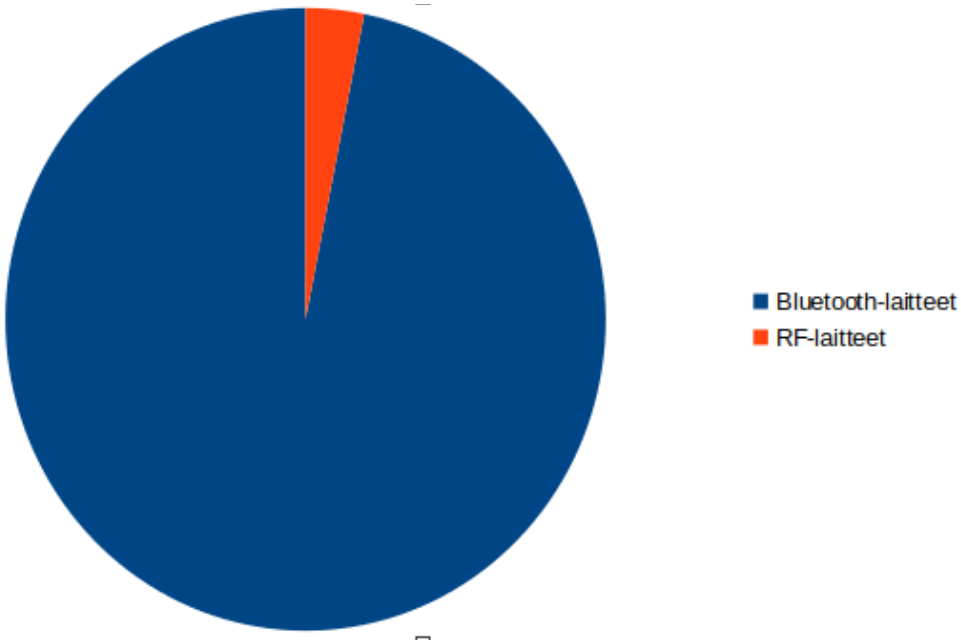
Primääriaineiston dataa kerättiin kahdella eri Wardriving kerralla. Niiden analyysi aloitetaan kronologisessa järjestyksessä ja lopuksi kerättyä dataa käsitellään yhtenäisenä kokonaisuutena. Analyysi tapahtuu tällä tavoin siksi, että se on selkeämpää ja ymmärrettävämpää kuin esimerkiksi kaiken aineiston esittäminen kerralla.

Primääriaineiston analyysin jälkeen tehdään haavoittuvuusarviota pohjaten primääri- ja sekundääriaineistoon sekä uusiin tietolähteisiin. Uusia tietolähteitä käytetään pääasiassa esimerkiksi Wardriving-tutkimuksessa löytyneiden IoT-laitteiden selvittämiseen. Uusien tietolähteiden käyttö on välttämätöntä haavoittuvuusarvioinnissa, sillä aikaisemman sekundääriaineiston perusteella ei voida välttämättä analysoida uusia löydöksiä, kuten esimerkiksi uusia IoT-laitteita.

Ensimmäisen ja toisen Wardrivingin analyysi aloitetaan käymällä läpi löytyneiden laitteiden määrää numeerisesti ja visuaalisesti. Visualisoinnissa käytetään apuna tilastollisia kaavoja sekä karttoja. Tämän jälkeen tuloksia analysoidaan pohjaten Wardrivingin aikana tehtyihin havaintoihin sekä sekundääriaineistoon.

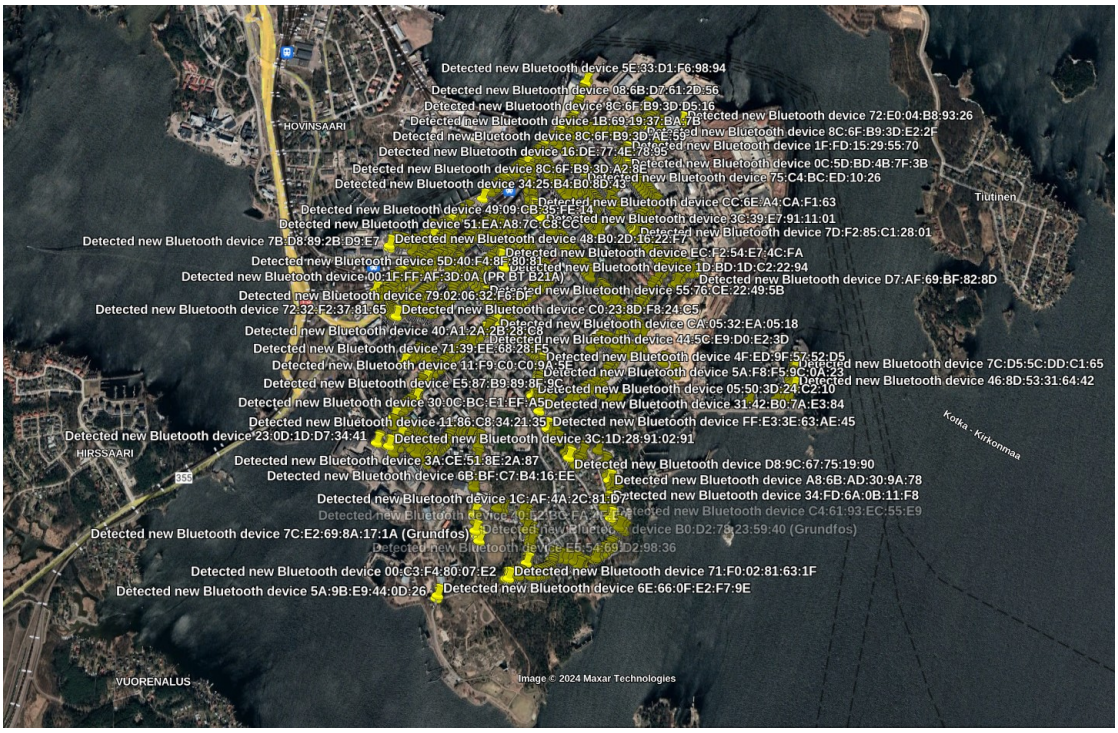
5.1 Primääriaineiston analyysi

Ensimmäisellä Wardriving-kerralla laitteita löytyi 3 738 kappaletta, joista suurin osa (96,8 %) oli Bluetooth-laitteita ja loput (3,2 %) niin kutsuttuja RF-laitteita eli RTL-SDR-vastaanottimilla havaittuja laitteita (kuva 15).



Kuva 15. Eri taajuuksilla lähettävien laitteiden osuudet

Ensimmäisellä Wardriving-kerralla löydetyt Bluetooth-laitteet eivät tallentuneet oikealla tavalla GPS-koordinaattien kanssa. Tiedot saatiin kuitenkin yhdisteltyä myöhemmin yksinkertaisella Python-skriptillä ja lopputuloksena saatiin kartta, jossa on massiivinen määrä Bluetooth-laitteita (kuva 16).



Kuva 16. Ilmakuva, jossa näkyy 3738 Bluetooth-laitetta (Google 2022)

Suurin osa löydetyistä Bluetooth-laitteista näyttää olevan laitteita, jotka eivät mainosta omaa nimeään. Sekundääriaineiston perusteella voidaan todeta, että tämä ilmiö johtuu todennäköisesti Bluetoothin MAC-osoitteiden randomisaatiosta. MAC-randomisaatio on implementoitu useisiin Bluetooth-laitteisiin ilmeisesti juuri siksi, että tämä estää esimerkiksi juuri Wardrivingilla suoritetun kyberstalkkaamisen.

Ilman MAC-osoitteiden randomisaatiota Wardrivingin avulla voitaisiin seurata laitteen olinpaikkaa. Tämä johtuu siitä, että pysyviä osoitteita voitaisiin käyttää yksilöivinä tunnisteina, joiden avulla laitteen liikkeitä voidaan seurata suorittamalla useita Wardriving-tutkimuksia. Selkeyden vuoksi kartalla onkin järkevämpää esitellä vain laitteet, jotka voidaan yksilöidä (kuva 17). Tämä saadaan kirjoittamalla uusi Python-skripti, joka poistaa aikaisemmin luodusta KML-tiedostosta kaikki laitteet, jotka sisältävät tiedoissaan pelkän MAC-osoitteen.

Kuva 17. Ilmakuva, jossa näkyy Bluetooth-laitteita, jotka sisältävät yksilöivän tunnuksen (Google 2022)

On kuitenkin mahdollista, että osa jäljelle jääneistä laitteista käyttää joka tapauksessa MAC-randomisaatiota, mutta laitteen nimi voi silti olla yksilöivä tekijä. Laitteita on jäljellä edelleen suuri määrä, joten kaikkia löydettyjä laitteita ei voida tutkia erikseen ajallisten rajoitteiden vuoksi. Tästä syystä kyseessä olevien laitteiden analyysi kohdistuu erityisesti ennalta määriteltyjen tärkeiden kohteiden alueille. Lisäksi analysoinnista karsitaan laitteita, joilla ei selvästi ole suurta merkitystä kyberturvallisuudelle.

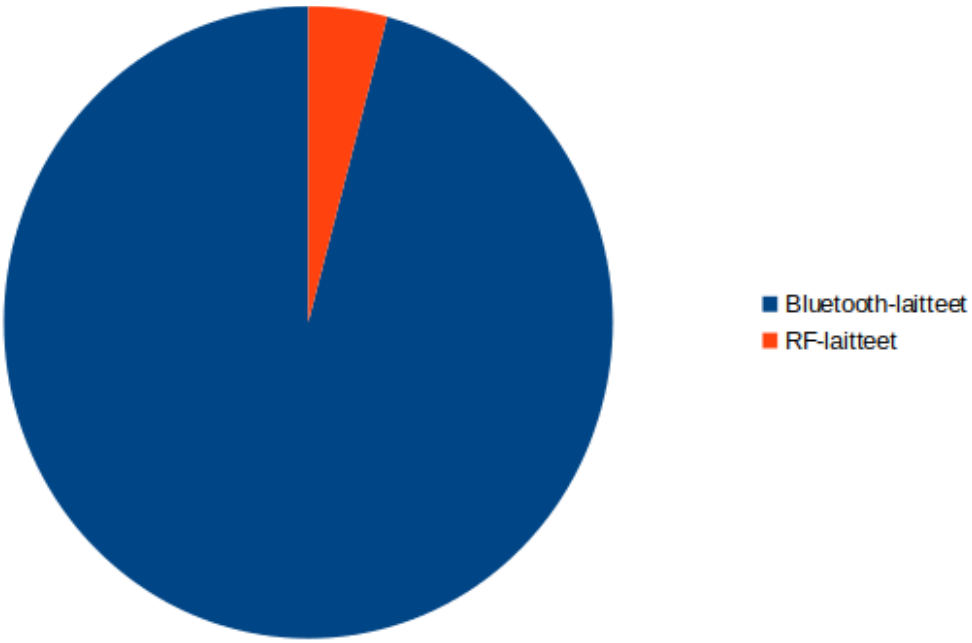
Toinen osa kerättyä primääriaineiston dataa ovat RF-laitteet. Näitä löytyi 121 kappaletta ja laitteet voidaan esittää kartalla suoraan (kuva 18). Nämä laitteet herättävät erityistä mielenkiintoa, sillä tutkimuksen aikana huomattiin, että laitteet käyttävät salausta vain harvoin. Tämä tarkoittaa sitä, että tiedonsiirto laitteiden välillä tapahtuu avoimessa muodossa ilman suojamekanismeja. Tämä johtaa siihen, että laitteiden hakkeroimiseen riittäisi yksinkertainen Replay-attack.

Replay-attack tarkoittaa tässä tapauksessa esimerkiksi sitä, että ensimmäiseksi hyökkääjä vastaanottaa laitteen lähettämän signaalin. Tämä voisi olla esimerkiksi langattoman autotallin oven avaussignaali. Hyökkääjä voi nyt tallentaa tämän kaappaamansa signaalin ja lähettää sen uudelleen esimerkiksi HackRF-ohjelmistoradiolla avaten itse kyseisen autotallin oven.

Kuva 18. Ilmakuva, jossa näkyy RF-laitteet, sekä ajettu reitti (Google 2022)

Toisella Wardriving-kerralla laitteita löytyi yhteensä 1 789. Määrä on pienempi kuin ensimmäisellä kerralla. Tätä voisi selittää se, että tällä kertaa ajettu reitti oli hieman erilainen (kuva 19). Suurin osa (95,6 %) oli Bluetooth-laitteita ja loput (4,4 %) niin kutsuttuja RF-laitteita (kuva 20). Eri laitetyyppien määrä on kuitenkin suhteessa samanlainen ensimmäisen Wardriving kerran kanssa.

Kuva 19. Ilmakuva, jossa näkyy toisella Wardiving kerralla ajettu reitti (Google 2022)



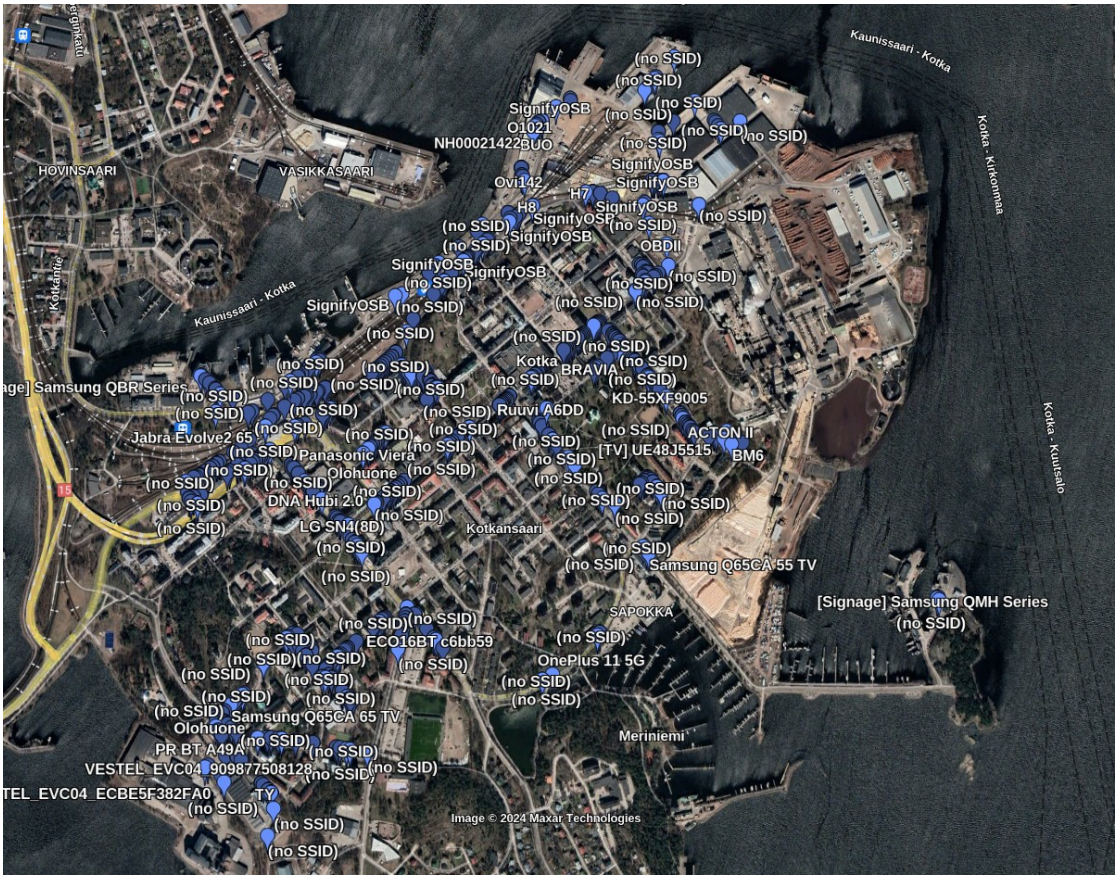
Kuva 20. Havainnollistava kuvakaavio eri taajuuksilla lähettävien laitteiden osuuksista.

Toisella Wardriving kerralla Kismet tallensi Bluetooth-laitteiden osalta dataa samalla tavalla eli ilman GPS-koordinaatteja. Aikaisemmin käytetyllä Python-

skriptillä saadaan kuitenkin luotua toimiva kartta myös tässä tapauksessa (Kuva 21).

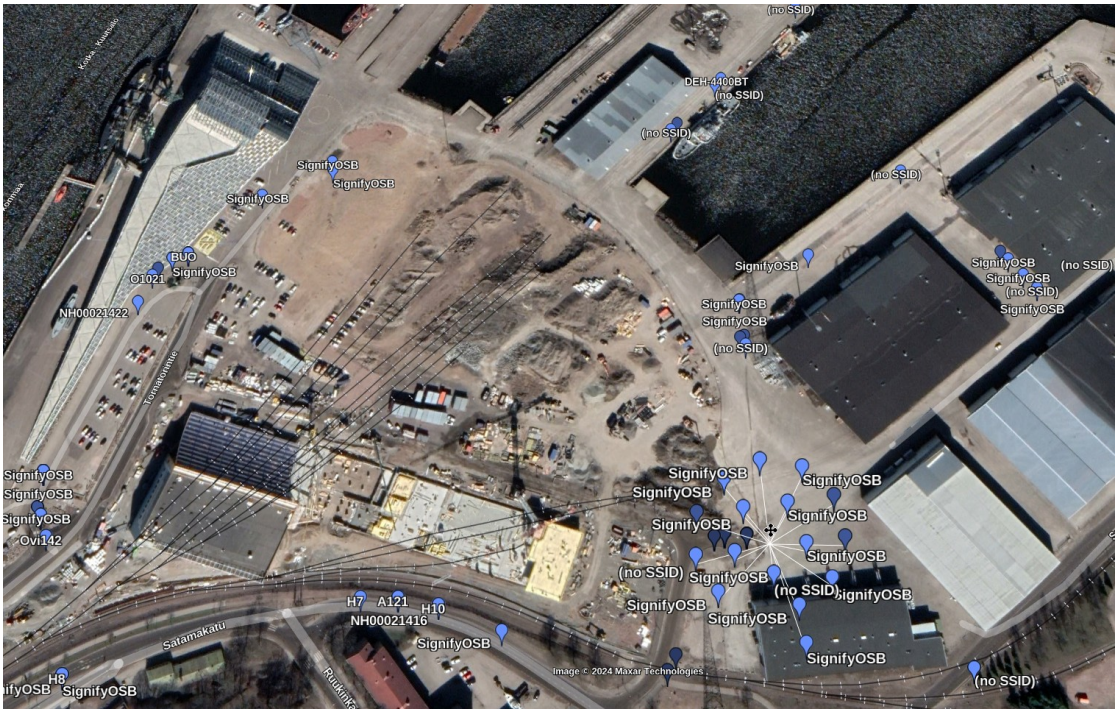
Kuva 21. Ilmakuva, jossa näkyy suodatetut Bluetooth-laitteet sekä ajettu reitti (Google 2022)

Kismetin lisäksi Bluetooth-laitteiden Wardrivingia suoritettiin Android-puhelimen ja WiGLE-sovelluksen avulla (kuva 22 ja kuva 23). Tällä tavoin saatiin dataa, jota voidaan verrata Kismetin tuloksiin. RF-laitteita löytyi tällä kerralla 78 kappaletta (kuva 24).



Kuva 22. Ilmakuva Kotkansaaresta ja WiGLEN:n avulla löydetyt Bluetooth-laitteet (Google 2022)

Bluetooth-laitteita löytyi WiGLE:n avulla hieman yli 900 kappaletta. Lisäksi moni Kismetin avulla aikaisemmin löytynyt laite löydettiin uudestaan. Tuloksen perusteella voidaan katsoa, että ainakin Bluetooth-dataa on kerätty oikein molemmilla Wardriving-kerroilla.



Kuva 23. Ilmakuva läheltä, kantasataman alueelta (Google 2022)

Kuva 24. Ilmakuva, jossa näkyy RF-laitteet sekä ajettu reitti (Google 2022)

Vertailemalla kahden Wardriving-tutkimuksen tuloksia keskenään voidaan tunnistaa trendejä tai poikkeamia, mikä lisää tutkimuksen luotettavuutta. Tulosten kerääminen on onnistunut molemmilla Wardriving-kerroilla, ja lisäksi voidaan havaita, että lopulliset tulokset ovat pääpiirteittäin samankaltaisia toistensa kanssa. Tämä vahvistaa, että tutkimuksen tulokset ovat luotettavia.

5.2 Löydettyjen laitteiden riskianalyysi

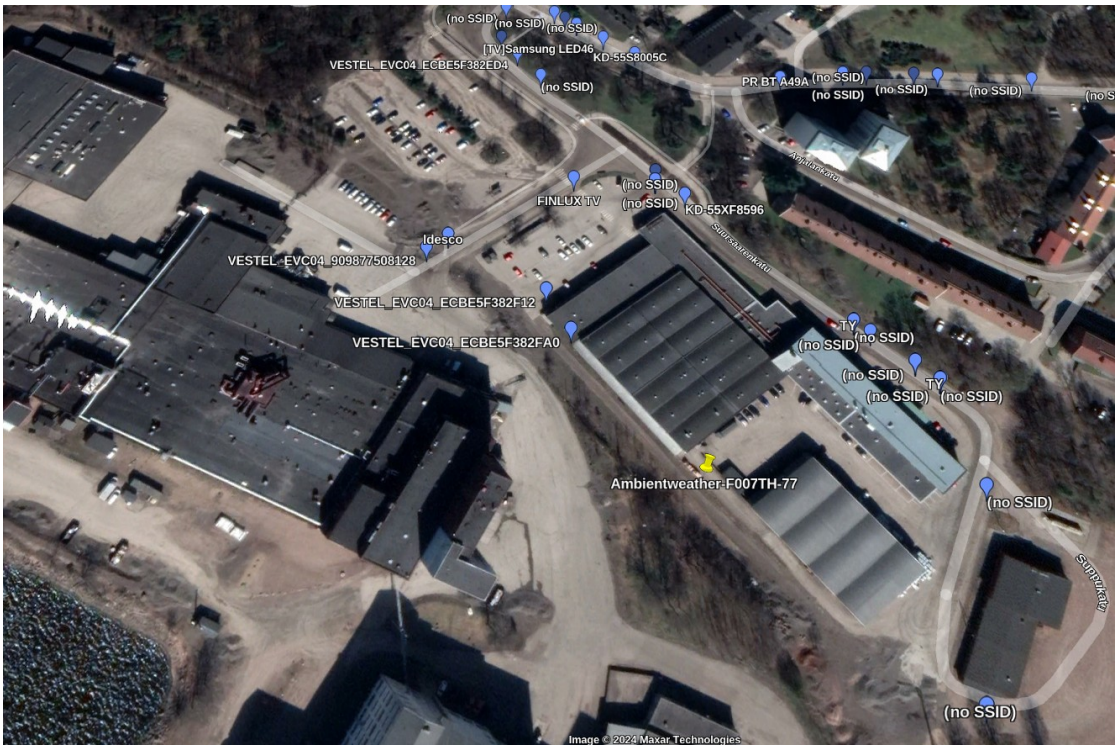
Löydettyjen laitteiden analysointi tehdään tutkimalla kaikkia Wardrivingin antamia tuloksia kerralla. Tämä on mahdollista siksi, että enää ei käsitellä esimerkiksi laitteiden lukumääriä tai muita arvoja, jotka voisivat haitata tulosten selkeyttä ja ymmärrettävyyttä. Laitteiden analysoinnissa käytetään paikan päällä otettuja kuvia löydetyistä laitteista Wardrivingin jälkeen. Tämä prosessi perustuu aiempiin tuloksiin, erityisesti aiemmin luotuihin karttoihin, jotka auttavat löytämään tässä osuudessa käsiteltäviä laitteita. Lisäksi kohteita tarkastellaan lähempää kartalla ja laitteiden nimien perustella etsitään tietoja esimerkiksi tunnetuista haavoittuvuuksista. Tunnettujen haavoittuvuuksien lähteenä hyödynnetään MITREn CVE-tietokantaa.

Laitteiden analyysi aloitetaan tärkeäksi määriteltyjen kohteiden alueilta (kuva 9). Ensimmäiseksi tärkeäksi määritelty kohde on Lantmännen Ceralia Kotka ja Hankkija Oy Kotkan Rehutehdas, eli analyysi aloitetaan siitä. Kohteesta löytyy Bluetooth-laitteet: ”VESTEL_EVC04”, ”FINLUX TV”, ”KD-55XF8596”, ”Idesco” ja ”TY” (kuva 25). RF-laitteistoa löytyy yksi kappale: ”Ambientweather-F007TH-77” (kuva 25).

Tässä kohtaa tarkemmasta analyysista jätetään pois: ”FINLUX TV”, ”KD-55XF8596”. Kokonaan jätetään pois laite nimeltä: ”TY”. Kaksi ensimmäistä laitetta ovat älytelevisioita ja viimeisen laitteen tiedoilla ei löydy tarpeeksi tietoa kyseisestä laitteesta. Lisäksi jätetään pois RF-laite nimeltä: ”Ambientweather-F007TH-77”.

Älytelevisioiden haavoittuvuudet eivät ole mitenkään ennekuulumattomia, mutta ne suodatetaan pois tarkemmasta analyysista tutkimuksen ajallisten rajoitteiden takia. Älytelevisiot ovat kuitenkin lyhyesti sanottuna laitteita, jotka voidaan yleensä saada haltuun helposti ja niiden avulla voidaan esimerkiksi tallentaa sekä ääntä että videota. Tämä voi olla erityisen suuri riski esimerkiksi yritysten kokoustiloissa, joissa keskustellaan salaisista aiheista. Tästä syystä älytelevisioita käsitellään analyysin jatkossa vain, jos ne näyttävät sijaitsevan erityisen kriittisissä kohteissa.

RF-laite: ”Ambientweather-F007TH-77” jätetään pois siksi, että internet-haun perusteella kyseessä on vain yksinkertainen lämpötila- ja kosteusanturi. Laite ei hyvin todennäköisesti ole käytössä esimerkiksi kriittisessä infrastruktuurissa tai muussa merkittävässä kohteessa, sillä laite ei selvästi ole tarkoitettu siihen (Ambientweather 2013).



Kuva 25. Ilmakuva, jossa näkyy ensimmäisen kohteen laitteet (Google 2022)

Aloitetaan tarkempi analyysi laitteesta: ”VESTEL_EVC04”, joita näyttää olevan useampi kappale kyseisellä alueella. Internet-haun perusteella löytyy nimeä vastaava sähköauton latausasema (kuva 26).

Kuva 26. Kuvakaappaus löydetyn latausaseman PDF-dokumentista (Finluxpro 2021)

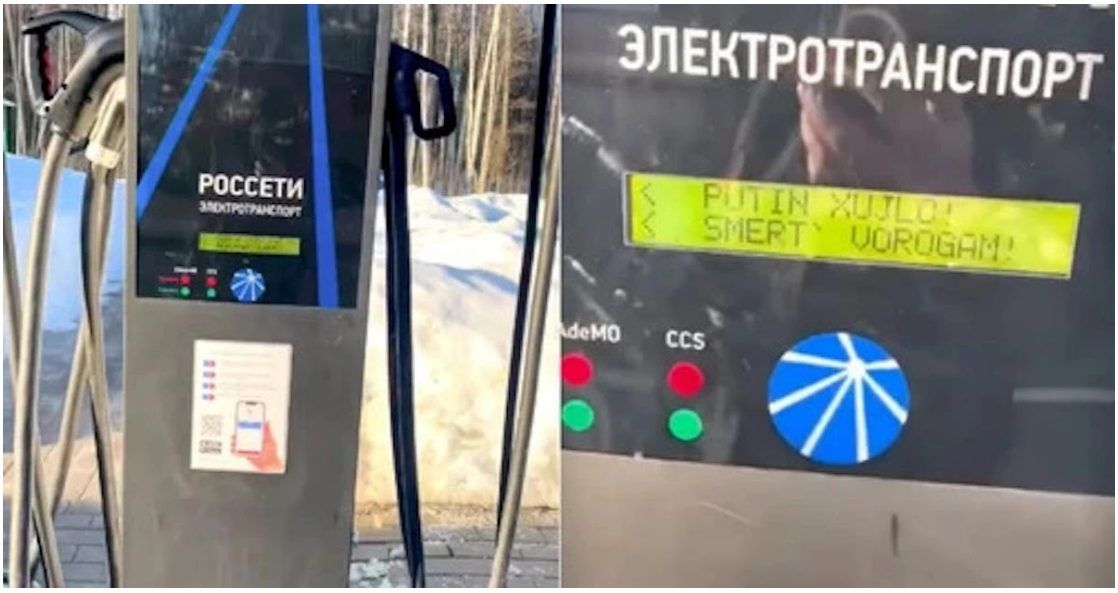
Internet-haun sekä CVE-tietokannan perusteella laitteelle ei löydy tunnettuja haavoittuvuuksia. Tämä ei kuitenkaan tarkoita sitä, että laite ei olisi haavoittuvainen hyökkäyksille. Dokumentaatioon perehdyttäessä voidaan huomata, että kyseinen laite käyttää ainakin Wi-Fiä ja RFID:tä kommunikoimiseen (Finluxpro 2021). Lisäksi Wardrivingin perusteella tiedetään, että laite käyttää myös Bluetoothia. Usean kommunikaatiotavan käyttö lisää merkittävästi laitteen hyökkäyspinta-alaa ja siksi voisi pitää todennäköisenä, että laite voisi olla haavoittuvainen jollekin hyökkäystavalle.

Dokumentaatiosta löytyy kuva kyseisestä laitteesta avattuna (kuva 27). Tämä voi antaa hyödyllistä tietoa laitteen ostajalle. Samalla se kuitenkin paljastaa tietoja laitteen toiminnasta. Kuvan avulla voidaan esimerkiksi päätellä, että miten latausasema voidaan avata ja mitä laitteistohakkerointia sille voisi tehdä. Laitteistohakkerointi vaatisi kuitenkin fyysistä kontaktia itse laitteeseen, mikä todennäköisesti vaikuttaa potentiaalisen hyökkääjän päätökseen. Kiinnijäämisriskiä voidaan kyseisessä tapauksessa pitää suurena.

Kuva 27. Kuva avatusta latausasemasta (Finluxpro 2021)

Yleisellä latausasemia koskevalla internet-haulla löytyy kuitenkin mielenkiintoisia tuloksia haavoittuvuuksista. Esimerkiksi Hackadayn artikkelin (2022) mukaan latausasemien valmistajat eivät ole panostaneet erityisen paljon laitteiden suojaamiseen. Tämä johtaa useisiin haavoittuvuuksiin, kuten siihen, että ohjelmistoradiolla voidaan kuunnella auton ja laturin välistä liikennettä sekä katkaista ajoneuvon lataaminen jopa 47 metrin etäisyydeltä. Lisäksi artikkelissa kerrotaan siitä, miten joistakin latausasemista voidaan saada haltuun koko latausaseman ohjelmisto. Tämä voisi tapahtua esimerkiksi käyttäen fyysistä sarjaporttiyhteyttä tai langatonta yhteyttä.

Hyvä esimerkki todellisesta hakkerointitilanteesta on Independentin artikkelissa (2022) kirjoitettu tapaus, jonka mukaan venäläisiä latausasemia on hakkeroitu niin, että ne ovat näyttäneet viestiä: ”Putin on munapää!” (kuva 28).



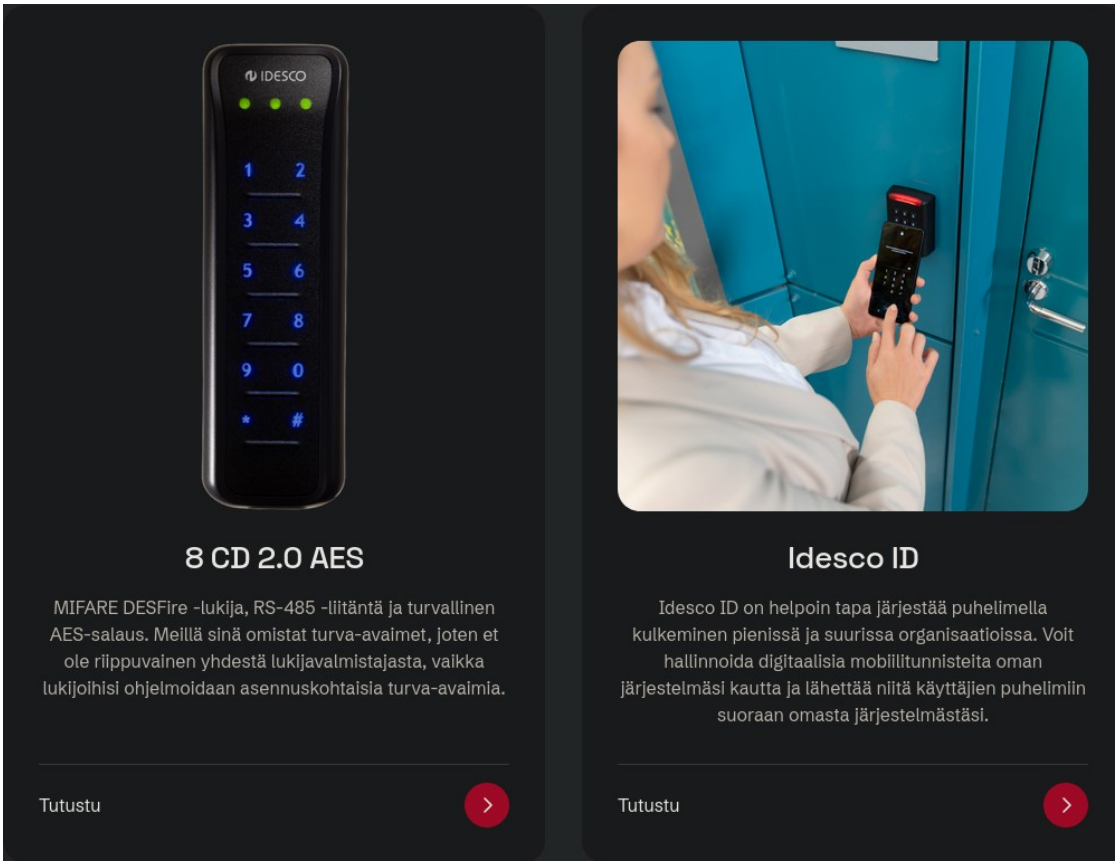
Kuva 28. Putinia solvaava latausasema (Massie 2022)

Latausasemien omistajat ovat kertoneet, että laitteet on rakennettu Ukrainassa, joka saattaa tarkoittaa sitä, että niihin on asennettu aikaisemmin takaportti (Massie 2022). Tässä tapauksessa motiivina on ollut todennäköisesti poliittinen vaikutus: arkipäiväisten asioiden hakkeroiminen saattaa aiheuttaa huolta ja jopa pelkoa Venäjän kansalaisissa

Edellä mainitut haavoittuvuudet saattavat kuulostaa siltä, että niitä voisi hyödyntää maksimissaan pieneen kiusantekoon. Tämä voikin olla totta, kun kyseessä on vain yksi latauslaite.

Useampaa laitetta ohjaamalla voitaisiin kuitenkin aiheuttaa jopa merkittävää sähköverkon horjumista, sillä latausasemat kykenevät kuluttamaan suuria määriä virtaa kerralla. Pelkästään usean, paljon virtaa käyttävän latausaseman irrottaminen samanaikaisesti voisi aiheuttaa sähköverkon horjumista tai jopa sen kaatumisen. Tämä on kuitenkin vielä toistaiseksi pelkkä teoreettinen uhka, mutta sähköautojen yleistyessä tämän teoreettisen uhan mahdollisuus luonnollisesti kasvaa. (Day 2022).

Toinen tarkemmin analysoitava laite on nimeltään: ”Idesco”. Internet-haun perusteella laite on todennäköisesti kulunvalvonnassa käytettävä RFID-lukija (kuva 29).



Kuva 29. Kuvakaappaus Idesco.fi -verkkosivustolta, jossa näkyy esimerkkejä mahdollisesta laitteesta (Idesco s.a.)

Wardrivingia suoritettaessa havaittiinkin, että tehtaiden pihassa on kulunvalvontaan liittyviä laitteita. Tiedossa ei ole kuitenkaan sen tarkempaa mallia, eli haavoittuvuuden etsiminen on vaikeaa. CVE-tietokannastakaan ei löytynyt tuloksia käyttämällä hakusanaa: ”Idesco”. Tämä valmistajan keino ilmoittaa pelkkä valmistajan nimi, mutta ei tarkkaa mallia on selvästi hyvä tapa ainakin hidastaa hyökkäyksen suunnittelua.

Yleisesti kulunvalvonnassa käytettäviä RFID-lukijoita on paljon erilaisia ja ne eroavat turvallisuuden kannalta toisistaan. Idescon verkkosivuja lukiessa käy ilmi, että käytännössä kaikki heidän valmistamat lukijat käyttävät salausta, joka vastaa nykyajan standardeja (Idesco s.a.). Salauksen käyttö estää ainakin yksinkertaisen RFID-tagien kopioimisen, joka lienee yleisin tapa väärinkäyttää RFID-kulunvalvontajärjestelmiä. Bluetooth-yhteys voisi avata mahdollisuuden väärinkäyttää lukijaa, mutta tätä ei voida tämän tutkimuksen avulla selvittää juuri puuttuvan sekundääriaineiston takia.

Yhteenvetona voidaan siis todeta, että kyseessä oleva lukija on todennäköisesti rakennettu kyberturvallisuutta ajatellen ja sen käyttö vaikuttaa olevan turvallista, mutta tätä ei voida yleistää kaikkiin RFID-lukijoihin.

Seuraava tärkeäksi määritelty kohde on Kotkan merivartioasema ja FinFerries autolautta. Kohteesta löytyy mielenkiintoisia laitteita: ”Toyota-xxxxxxxx” (kuva 30). Näitä laitteita näyttää siis olevan useampi. Muut laitteet jätetään tarkemman analyysin ulkopuolelle, koska ne joko on jo aiemmin päätetty poistettavaksi tai ne ovat samantyyppisiä kuin aiemmin seulotut laitteet. Perustelut tälle ovat siis samanlaisia kuin aikaisemmin, joten niitä ei selkeyden vuoksi eritellä enää erikseen.

Kuva 30. Ilmakuva, jossa näkyy toisen merkittävän kohteen laitteet (Google 2022)

Analysoitavaksi laitteeksi valitaan: ”Toyota-xxxxxxxx”. Internet-haun perustella löytyy vastaava laite, eli auton langaton rengaspainemittari (kuva 31).

Kuva 31. Toyotan langaton rengaspainemittari (Clifford 2022)

Toyota UK Magazinen artikkelin (Clifford 2022) mukaan laite ilmoittaa auton kuljettajalle, jos renkaasta alkaa hävitä painetta. Lisäksi artikkelissa kerrotaan, että tämä ominaisuus on tullut pakolliseksi Euroopassa vuonna 2014. Tämä tarkoittaa käytännössä sitä, että analysoitavat asiat koskevat kasvavissa määrin ainakin eurooppalaisia henkilöautojen omistajia.

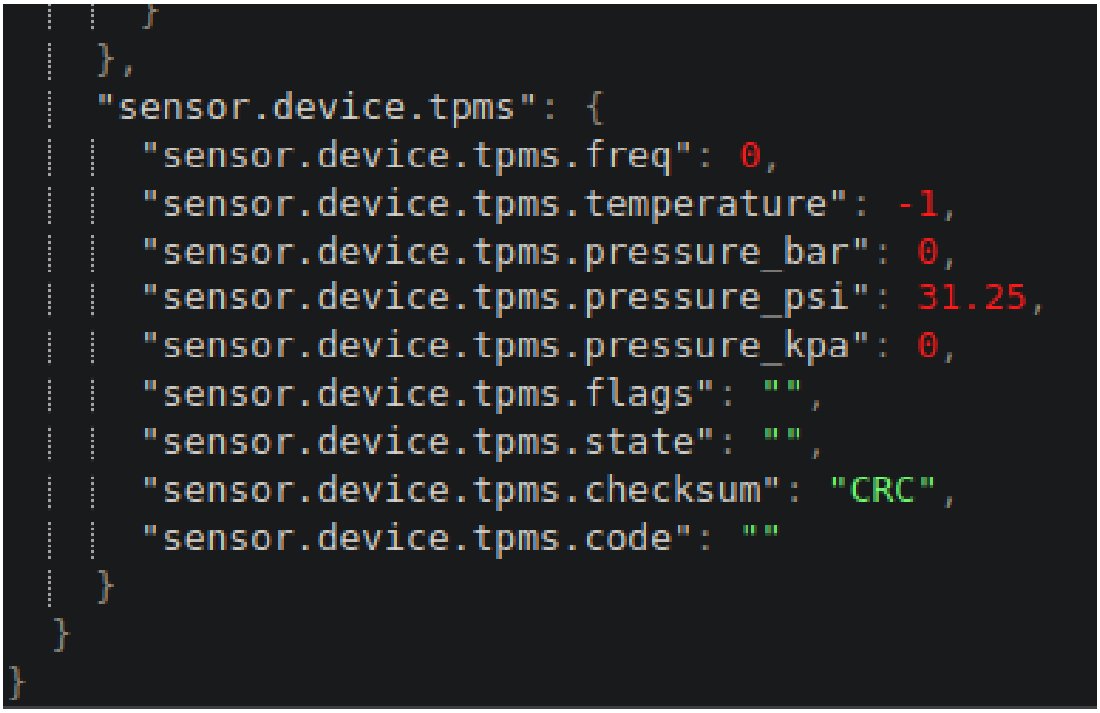
CVE-tietokannasta ei löydy suoraa haavoittuvuutta laitteelle. Yleisellä internet-haulla mittareista löytyy kuitenkin RTL-SDR-blogin artikkeli (2017) jonka mukaan rengaspainemittarit ovat haavoittuvaisia hyökkäykselle. Käytännössä hyökkäys toimii niin, että esimerkiksi HackRF-ohjelmistoradiolla kaapataan mittarin lähettämää dataa. Tämän jälkeen data analysoidaan ja analysoidun datan avulla voidaan nyt lähettää itse dataa, jota henkilöauto luulee mittarin lähettämäksi.

Tällä tavoin autolle voidaan lähettää esimerkiksi väärää tietoa siitä, että rengas olisi yhtäkkiä tyhjä. Auton ilmoitus tyhjästä renkaasta saisi todennäköisesti kuljettajan pysäyttämään autonsa. Tämä taas voi aiheuttaa tarpeetonta vaaraa tiellä liikkuville sekä häiritä kuljettajan matkaa ilman todellista syytä. Lisäksi jos väärä hälytys toistuu usein, se voi heikentää kuljettajan luottamusta auton järjestelmiin ja aiheuttaa epäluottamusta auton varoitusjärjestelmien toimintaa kohtaan. Auton matkustajia vastaan hyökkäävä

osapuoli voisi käyttää pysähtymistä hyväksi esimerkiksi henkilöiden estämiseen, ryöstöön tai muuhun rikolliseen toimintaan.

Toinen ehkä omalla tavallaan vakavampi ongelma löytyy RTL-SDR-blogin artikkelin (2017) perusteella siitä, että esimerkiksi traktorit käyttävät samanlaisia mittareita renkaiden automaattiseen paineen säätelyyn. Artikkelin mukaan väärä ilmoitus alhaisesta rengaspaineesta saattaisi aiheuttaa renkaiden liiallisen täyttymisen, joka voisi johtaa renkaan vahingoittumiseen.

Kismetin keräämää dataa tutkimalla voidaan myös havaita, että renkaat ilmoittavat yksilöivän id:n, renkaan lämpötilan ja rengaspaineen (kuva 32). Yksilöivä id on nähtävissä heti löydetyn laitteen nimestä.



Kuva 32. Kismetin tallentamaa dataa rengaspainemittarista

Näitä tietoja hyödyntämällä voidaan päätellä monenlaisia asioita. Yksilöivän tunnisteen käyttö mahdollistaa auton tunnistamisen sekä auton liikkeiden seuraamisen, mikä voi johtaa kohdennettuihin rikoksiin, kuten varkauksiin tai seurannan avulla toteutettuihin hyökkäyksiin.

Renkaan lämpötila- ja painetiedot voivat puolestaan paljastaa lisää tietoja auton käytöstä. Voidaan esimerkiksi päätellä, että tarpeeksi kauan paikalla seisseen auton renkaiden lämpötila on kutakuinkin sama, kuin ympäröivän

ilman lämpötila. Tästä ja kitkan vaikutuksesta lämpötilaan voidaan päätellä, että lämpimämmät renkaat viittaisivat siihen, että autolla on ajettu lähiaikoina. Huoneilmaa tai hieman matalampaa lämpötilaa vastaava lämpötila-arvo voi puolestaan viitata siihen, että autoa säilytetään esimerkiksi lämmitetyssä autotallissa. Kaasujen kinetiikan lakien perusteella tiedetään myös, että paine kasvaa, kun lämpötila nousee. Näitä arvoja vertailemalla voidaan saada yllättävänkin yksityiskohtaista tietoa auton käytöstä.

Seuraavaksi siirrytään kolmanteen kohteeseen, eli Kotkamills ja Kantasataman alue. Kotkamillssin alueelle (kuva 33) ei päästy suorittamaan Wardrivingia, sillä alue on suljettu. Tästä syystä tarkempi analyysi siirretään suoraan Kantasataman alueelle.

Kuva 33. Ilmakuva Kotkamillsin alueesta (Google 2022)

Kantasataman alueelta löytyy seuraavat kiinnostavat laitteet: ”SignifyOSB” ja ”Seos” (kuva 34). Tälläkin kertaa laitteita on suodatettu pois selkeyden sekä aikaisemmin määriteltyjen seikkojen vuoksi.

Kuva 34. Ilmakuva Kantasataman alueesta, jossa näkyy löydetyt laitteet sekä ajettu reitti (Google 2022)

Analyysi aloitetaan laitteesta ”SignifyOSB”. Internet-haulla löytyy laitevalmistaja ”Signify” joka on entinen ”Phlips Lightning” (Signify s.a.). Sivuston perusteella saadaan tietää, että Signify tuottaa älykkäitä valaisuratkaisuja.

Pelkkä nimi ei paljasta tarpeeksi laitteesta, eli tarkempaan analyysiin tarvitaan lisätietoja. Tästä syystä analyysiä jatkettiin menemällä paikan päälle etsimään kyseistä laitetta (kuva 35). Paikan päällä käyminen tulosten perusteella ja laitteen löytäminen on myös erinomainen tapa osoittaa tutkimuksen tulosten luotettavuutta.

Kuva 35. Katulamppu, joka mainostaa itseään Bluetoothin avulla käyttäen nimeä: ”SignifyOSB”

Saman nimisiä laitteita löytyi esimerkiksi Kismetin ja toisen Wardriving kerran yhteydessä 134 kappaletta. Paikan päällä havaittiinkin, että laitteita on useita (kuva 36). Tämä on konkreettinen todiste siitä, että Wardrivingin avulla saadut tulokset vastaavat pitkälti reaalimaailman tilannetta.

Kuva 36. Kuvassa useampi SignifyOSB-katulamppu

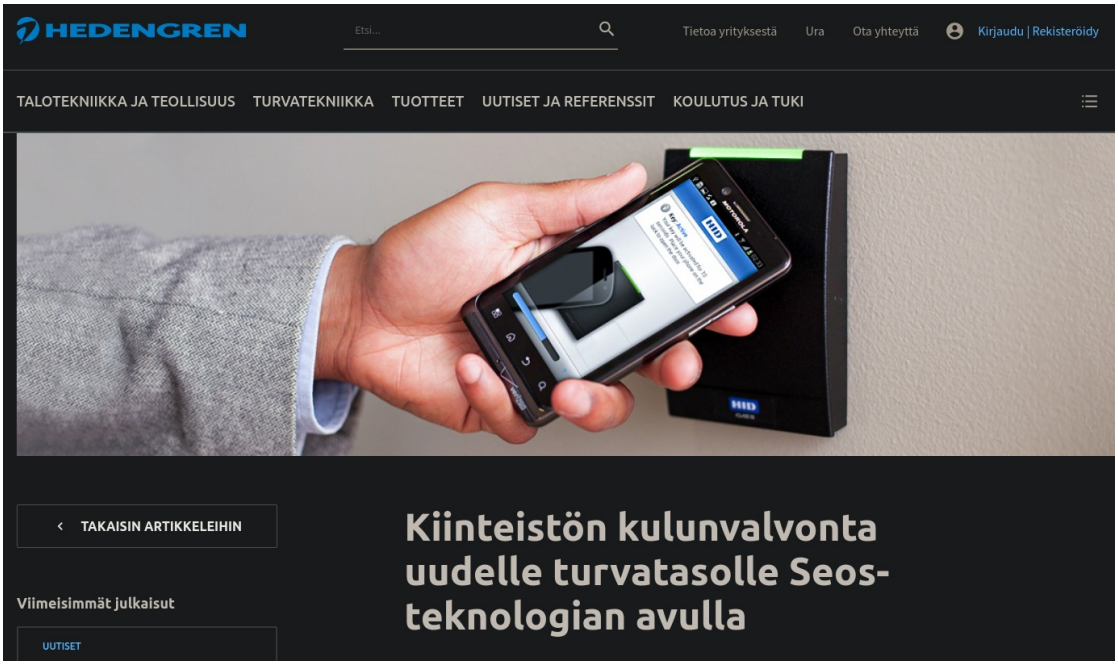
CVE-tietokannasta löytyy hakusanalla ”Signify” haavoittuvuus, jonka CVE-ID on ”CVE-2019-18980” (Mitre 2023). Laite ei vastaa Wardrivingin avulla löydettyä laitetta, mutta se antaa osviittaa saman valmistajan käyttämistä toimintatavoista.

Kyseisessä laitteessa suojaamaton ohjelmointirajapinta mahdollistaa lampun käyttämisen etänä. Kuka tahansa voi siis etäkäyttää lamppua

sammuttaakseen tai sytyttääkseen sen tai vaihtaakseen sen väriä tai kirkkautta. Rajapinnan käyttämiseen ei vaadita tunnistautumista tai salausta. Ainoa vaatimus on, että hyökkääjällä on yhteys verkon kautta lamppuun. (Mitre 2023). Haavoittuvuuden triviaalisuus viittaa siihen, että Signify ei ehkä aseta kyberturvallisuutta etusijalle laitteidensa valmistuksessa.

Tämän tyyppiset haavoittuvuudet voivat altistaa useille haitaillisille seurauksille, jotka vaihtelevat valon ohjauksen häiriöistä aina fyysiseen vaaraan asti. Kantasataman tapauksessa hyvän valaistuksen voidaan olettaa olevan tärkeää, sillä satamassa on paljon erilaista liikennettä. Liikenteen häiriintyminen saattaa aiheuttaa vaaratilanteita ja viivästyksiä, mikä puolestaan voi johtaa merkittäviin taloudellisiin menetyksiin. Lisäksi huonosti valaistu satama-alue voi houkutella rikollisia toimimaan alueella, mikä lisää varkaus- ja turvallisuusriskiä alusten ja lastin suhteen.

Toinen tarkemmin analysoitava laite on nimeltään: ”Seos”. Internet-haun perusteella laite on todennäköisesti kulunvalvonnassa käytettävä Bluetooth/NFC-lukija (Hedengren 2017) (kuva 37).



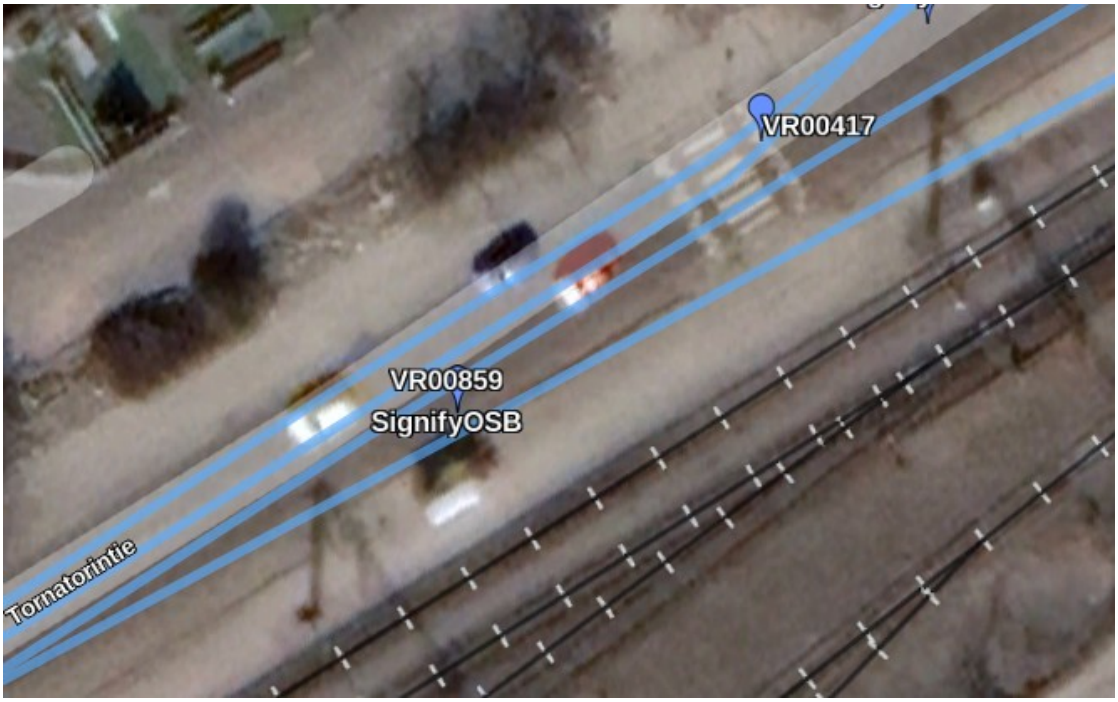
Kuva 37. Kuvakaappaus internet-haun tuloksesta (Hedengren s.a.)

Myös tämän kulunvalvontalaitteen osalta voidaan soveltaa aiempaa pohdintaa kulunvalvonnan kyberturvallisuudesta. Lyhyesti, laitteiden turvallisuus riippuu

vahvasti sen valmistajan määrittämistä ominaisuuksista. Tässä tapauksessa valmistaja tarjoaa uusia päivityksiä sekä salausominaisuutta, joka estää tunnistekorttien kopioimisen (Hedengren 2017). Lisäksi yleisellä internet-haulla ei löydy haavoittuvuuksia laitteesta. CVE-tietokannastakaan ei löydy haavoittuvuutta kyseiselle laitteelle, joten analyysissä voidaan siirtyä viimeiseen merkittäväksi määriteltyyn kohteeseen.

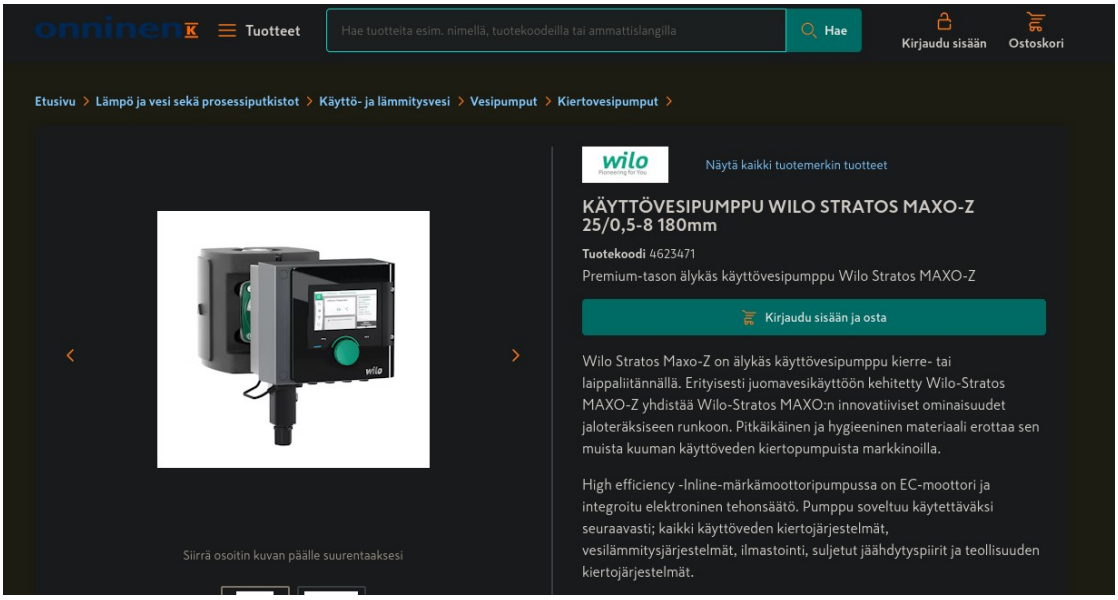
Viimeinen analysoitava merkittävä kohde on Kotkan Sataman juna-asema ja Kotkan rautatieasema. Alueelta löytyy kiinnostavia laitteita, jotka ovat nimeltään: ”Stratos MAXO-Z 25/0,5-8” ja ”Vrxxxxx” (kuva 38 ja kuva 39).

Kuva 38. Ilmakuva, jossa näkyy laitteen: ”Stratos MAXO-Z 25/0,5-8” sijainti (Google 2022)



Kuva 39. Ilmakuva, jossa näkyy laitteen: ”VRxxxxx” sijainti (Google 2022)

Ensimmäinen laite: ”Stratos MAXO-Z 25/0,5-8” vaikuttaa internet-haun perusteella olevan korkean tason käyttövesipumppu (Onninen s.a.) (kuva 40). Laite on tarkoitettu erityisesti juomavesikäyttöön (Onninen s.a.). Voidaan siis sanoa, että laitetta käytetään osana kriittistä infrastruktuuria. Google Earthin katunäkymää tarkasteltaessa voidaankin havaita, että laite on todennäköisemmin käytössä viereisten kerrostalojen juomaveden pumppaamossa (kuva 41). Kyseisen laitteen lisäksi löytyy muitakin pumppuja. Ne ovat nimeltään: ”Grundfos”, mutta ajallisten resurssien vuoksi tarkemmassa analyysissa käsitellään vain yhtä pumppua.



Kuva 40. Kuvakaappaus Onnisen verkkosivuilta, jossa näkyy löydetty laite (Onninen s.a)

Kuva 41. Google Earthin katunäkymästä otettu kuvakaappaus, jossa näkyy luultavasti vesipumppaamo (Google 2022)

CVE-tietokannasta ei löydy haavoittuvuuksia kyseiselle laitteelle. Tarkemmalla sekundääridatan analysoinnilla voidaan kuitenkin havaita, että kyseisen

laitteen Bluetooth-moduulille on määrätty toimintaohjeet, joiden mukaan voidaan muokata Bluetooth-yhteyden käyttäytymistä (Wilo 2022).

Ohjeiden mukaan seuraavat asetukset voidaan tehdä valikon kautta (Wilo 2022):

1. Bluetooth – PÄÄLLÄ/POIS
   Wilo-Smart Connect -moduulin BT Bluetooth-signaali voidaan kytkeä päälle tai pois päältä. Jos signaali on pois päältä, yhteyttä moduuliin ei voi muodostaa.

2. Yhdistettävyys – PÄÄLLÄ/POIS
   Yhteyden muodostaminen voidaan estää asettamalla tämä toiminto "OFF"-asentoon. Moduuli voidaan kuitenkin löytää Bluetooth-haulla.

3. Dynaaminen PIN-koodi – PÄÄLLÄ/POIS
   Yhteyden muodostaminen mobiililaitteesta tuotteen hallitsemiseksi vaatii tunnistautumiseen PIN-koodin syöttämisen.
   ON:
   Uusi PIN-koodi luodaan aina dynaamisesti ja näytetään tuotteen näytössä joka kerta, kun yhteys muodostetaan.
   OFF:
   Joka kerta yhteyden muodostamisen yhteydessä viimeiset neljä numeroa Wilo-Smart Connect -moduulin BT-sarjanumerosta käytetään PIN-koodina. Sarjanumero on painettu Wilo-Smart Connect -moduulin BT-arvokilpeen. Tätä kutsutaan "staattiseksi PIN-koodiksi".
   Kuvassa 1 on esitetty arvokilpi Smart Connect -moduulille BT. Tässä esimerkissä moduulin "staattinen PIN-koodi" on 6789.

Ohjeiden sekä Wardriving-tulosten avulla voidaan päätellä, että Bluetooth on päällä. Tämän perusteella ei voida kuitenkaan tietää, että onko toisen kohdan yhteys moduuliin sallittu tai ei, sillä moduuli voidaan joka tapauksessa löytää Bluetoothin avulla. Kolmannen kohdan PIN-koodi voi olla asetettu pois tai päälle. PIN-koodin asettaminen voisi hidastaa mahdollisen hyökkääjän yhteyttä laitteeseen.

Tämä on kuitenkin heikko tapa suojata laitetta, sillä nelinumeroisen Bluetooth-PIN-koodin murtaminen on mahdollista alle 0,3 sekunnissa. Kaiken lisäksi tämän todistavassa tutkimuksessa käytettiin nykystandardeilla erittäin hidasta: ”Pentium III 450 MHz” prosessoria. (Shaked, Y., ym). Lisäksi PIN-koodi voi muodostua laitteen arvokilven loppuosasta, joka saattaa olla pääteltävissä tai havaittavissa esimerkiksi tutkiessa laitetta paikan päällä.

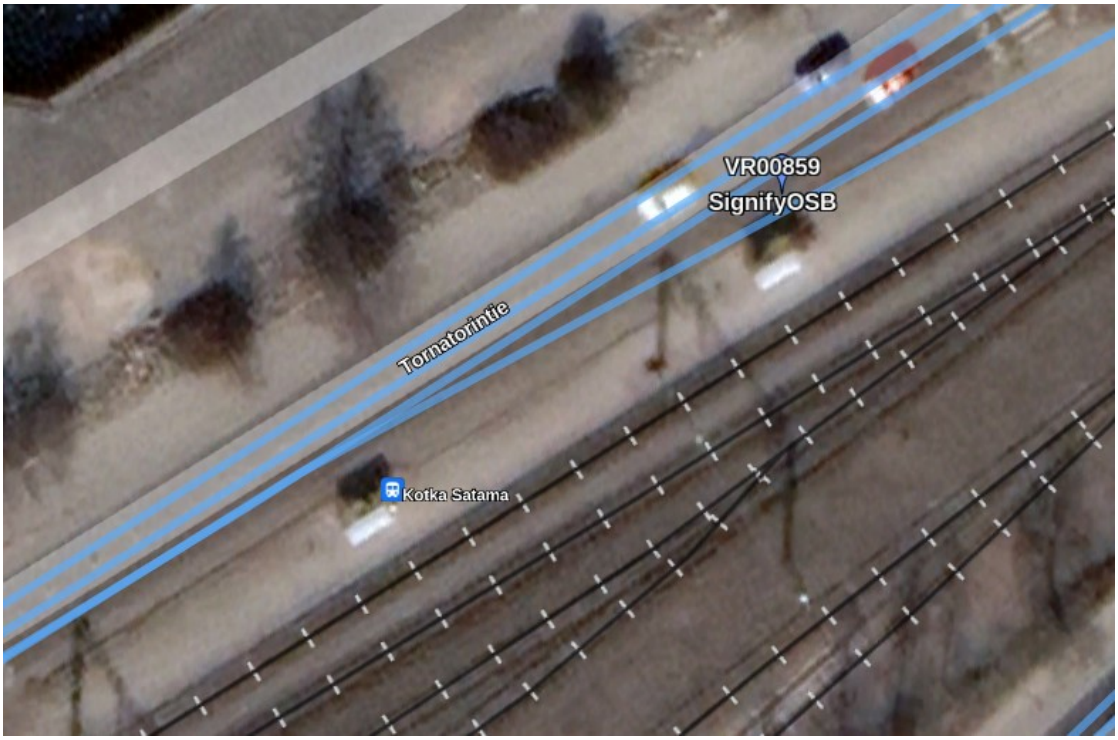
Laite käyttää myös useampaa langatonta rajapintaa viestinnässään. Laite saattaa siis paljastaa arvokilpensä numeron joissakin näistä rajapinnoissa. PIN-koodin ohittaminen saattaisi myös onnistua yksinkertaisesti sillä, että laitteeseen yhdistetään automaattisesti tuhansia kertoja ja joka kerta käytetään samaa koodia, vaikka 1234. Pumppu arpoisi jokaisella kerralla uuden numeron, ja jossain vaiheessa koodi olisi 1234.

Laitteet halutaan tehdä usein helpoiksi käyttää ja tämä johtaa siihen, että laitteelle ennalta määritellyt asetukset ovat heikot. On siis todennäköistä, että kyseessä olevan vesipumpun asetukset ovat tälläkin hetkellä sellaiset, että kuka vaan voi muodostaa yhteyden laitteeseen. Joka tapauksessa, jos aiempi teoreettinen haavoittuvuusanalyysi osoittautuisi todeksi, pumpun käyttämät suojauskeinot ovat parhaimmillaankin heikkoja.

Käyttövesipumpun hakkeroimisen seuraukset voisivat olla hyvin vakavia. Hyökkääjä voisi esimerkiksi muuttaa pumpun toimintaa ja asetuksia. Tämä voi johtaa veden virtauksen muuttumiseen joko liian suureksi tai liian pieneksi, mikä saattaa aiheuttaa putkistojen vaurioita tai vedenjakeluongelmia. Pahimmillaan tämä voisi johtaa veden saannin katkeamiseen kokonaan, mikä vaarantaa asukkaiden terveyden ja turvallisuuden.

Lisäksi hyökkäykseen voisi liittää esimerkiksi ransomware-hyökkäyksen. Hyökkääjä voi vaatia lunnaita käyttövesipumpun palauttamiseksi normaaliin toimintaan. Tämä voi aiheuttaa taloudellisia tappioita ja häiriöitä käyttäjille. Käyttövesipumpun hakkeroiminen voi johtaa myös luottamuksen menetykseen vedenjakelujärjestelmiä kohtaan ja herättää kysymyksiä vedenjakelun turvallisuudesta. Tämä voisi vaikuttaa yhteiskunnan vakauteen sekä talouteen.

Toisesta laitteesta: ”VRxxxxx” ei löydy CVE-tietokannasta tai internet-haulla mitään. Laitetta voidaan kuitenkin pitää kiinnostavana, koska sen sijainti viittaa siihen, että se liittyy jollain tavalla VR:n junaan (kuva 42). Tämä on kiinnostavaa siksi, että julkinen liikenne liittyy kriittiseen infrastruktuuriin.



Kuva 42. Ilmakuva laitteen: ”VRxxxxx” sijainnista

Laitteesta ei kuitenkaan näytä löytyvän tietoa mistään internetin lähteistä. Tästä syystä kohdetta mentiin tutkimaan myöhemmin paikan päälle. Paikan päällä havaittiin, että VR:n pysäkkejä on kaksi kappaletta. VRxxxx-laitteita näyttää tulosten perusteella olevan myös kaksi kappaletta. Wardrivingia suorittaessa havaittiin, että junia oli asemalla vain yksi kerrallaan, mutta vaunuja saattoi olla useampi. Näistä syistä tuloksista ei voida päätellä sitä, että onko VRxxxxx-laitteiden lähteenä esimerkiksi pysäkit tai junat.

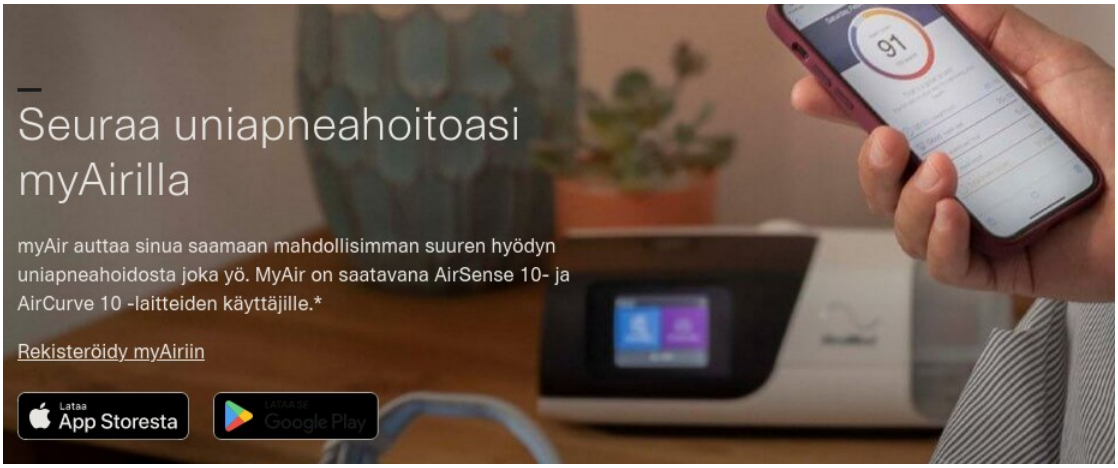
Sekundääriaineiston puutteellisuuden vuoksi voidaan vain arvailla kyseisten laitteiden käyttötarkoitusta. Laitteet voivat olla esimerkiksi lähettimiä, joiden avulla kuulovammainen voi kuulla junien kuulutuksia. Tästä ei kuitenkaan löytynyt minkäänlaisia lähteitä, joka olisi tässä tapauksessa outoa, sillä yleensä tällainen tieto olisi hyvin dokumentoitua.

Toinen arvaus on, että laitteet voivat liittyä junien seurantaan. Kyseessä olisi tällöin Bluetooth-beaconeiden käyttö, eli käytännössä tunnistetietojen jakaminen. Tällaisessa tapauksessa tunnistetietoja olisi helppo väärentää, jonka avulla voitaisiin vaikuttaa junien paikkatietoihin. Kummallekaan spekuloinnille ei kuitenkaan löytynyt VR:ää koskevia lähteitä, joten tarkempi analyysi päätettiin lopettaa tämän laitteen osalta.

Tärkeiden kohteiden alueilta tunnistettiin mielenkiintoisia laitteita, joista monet vaikuttivat liittyvän kriittiseen infrastruktuuriin. Analysoitujen laitteiden osalta havaittiin lähes jokaisessa kehityskohtia, joita olisi mahdollista parantaa. Vaikka MITREn CVE-tietokannasta ei suoraan löytynyt haavoittuvuuksia näille laitteille (Mitre 2023), yleisellä internet-haulla löydettiin useista laitteista kiinnostavaa tietoa. Mikäli haavoittuvuuksia löytyi, olivat ne myös yleensä vakavia. Riskit olivat merkittäviä sekä teoreettisesti että käytännössä.

Wardrivingin avulla kerättiin dataa myös muilta Kotkansaaren alueilta. Tästä syystä tarkempaa analyysiä jatketaan myös muiden alueiden osalta. Ajallisten resurssien sekä massiivisen datamäärän takia seuraavaksi analysoitavat laitteet on valittu osittain satunnaisesti. Otannassa on kuitenkin huomioitu sekundääriaineiston lisäksi myös muu tutkimuksen aikana hankittu tieto ja havainnot.

Ensimmäinen satunnaisotannasta poimittu laite on nimeltään: ”ResMed xxxxxx”. Kyseessä on internet-haun perusteella uniapneaan tai hengityshoitoon käytettävä laite (ResMed s.a.). Laitteita löytyy toisen Wardriving-kerran avulla kuusi kappaletta. Laitteet mainostavat lisäksi kuusinumeroista lukua, mutta tämän perusteella ei kuitenkaan voitu määrittää tarkkaa mallia. Tästä syystä tarkemmin analysoitavaksi laitteeksi valitaan laite, joka voisi hyvin olla yksi näistä löydetyistä laitteista (kuva 43).



Kuva 43. Kuva uniapnean hoitoon käytettävästä laitteesta ja sovelluksesta (ResMed s.a.)

Laite voidaan yhdistää sovellukseen nimeltä: ”myAir” joka ilmeisesti on syy sille, että kyseinen laite käyttää Bluetooth-yhteyttä. CVE-tietokannasta ei löydy erillisiä haavoittuvuuksia laitteelle tai ”myAir”-sovellukselle. Yleisen internet-haun perusteella laitteesta ei löydy tunnettuja haavoittuvuuksia.

Laitevalmistaja näyttää kuuluvan ”HackerOne”-haavoittuvuuksien palkkio-ohjelmaan, mikä kertoo siitä, että yritys ottaa kyberturvallisuuden vakavissaan (HackerOne s.a.). Tämä voi osittain selittää, miksi ResMedin laitteista ei ole löydetty ainakaan merkittäviä hakkerointitapauksia. Toisaalta laitteesta löytyy blogipostaus, josta käy ilmi, että laite on mahdollista ”jailbreakata” eli poistaa valmistajan asettamia rajoituksia (Airbreak 2020).

Tämä tarkoittaa käytännössä sitä, että laitteessa voidaan tällöin suorittaa omaa koodia ilman rajoituksia. Itse jailbreakkaaminen onnistuu käytännössä vain, jos laitteen käyttöjärjestelmässä on jokin haavoittuvuus, joka mahdollistaa oman koodin suorittamisen korotetuilla oikeuksilla (Kaspersky s.a.). Tämä puolestaan kertoo siitä, että laite ei ole täysin turvallinen – mikä ei kuitenkaan ole harvinaista älylaitteiden keskuudessa.

Laitteesta ei siis löydy tiedossa olevia haavoittuvuuksia, jotka voisivat vaarantaa käyttäjän turvallisuuden. Toisaalta tämä ei ole mikään vakuutus laitteen turvallisuudesta. Esimerkiksi laitteen nimen jatkuva mainostaminen Bluetoothilla ei ole ehkä aivan nykyaikaisten hyvien kyberturvallisuuskäytäntöjen mukaista. Nimen mainostaminen altistaa juuri esimerkiksi Wardrivingin tuomille uhkille. Tässä tapauksessa voidaan

esimerkiksi arvioida erittäin tarkasti laitteen sijaintia, joka voisi johtaa siihen, että tulevaisuudessa mahdollisesti esiin tulevat haavoittuvuudet on helppo kohdistaa laitteen käyttäjiin. Lisäksi laitteen sijainnin avulla voitaisiin tehdä erittäin uskottavia sosiaalisen manipuloinnin (eng. social engineering) hyökkäyksiä. Hyökkäyksen kohteena olevalle henkilölle voitaisiin esimerkiksi soittaa ja esittää hänen lääkäriään. Kuka muu tietäisi muka yhtä tarkasti, että mitä lääketieteellistä laitetta käytät kotonasi?

Toinen käsiteltävä laite, joka on valittu satunnaisotannan joukosta, on nimeltään: ”Secplus-v1-2133”. Kyseessä on yleisen internet-haun perusteella autotallin oven avaaja, joka toimii langattomasti (Github s.a.) (kuva 44).

Kuva 44. Esimerkkikuva autotallin ovesta ja sen avaajasta (Automaticgaragesolutions.com. 2017)

Sekundääriaineiston perusteella ”Secplus-v1” on geneerinen laite, joka voi olla useammassa erilaisessa autotallin oven avaajassa. Kyseessä on siis tarkemmin autotallin oven ohjausyksikkö (Github s.a.).

CVE-tietokannasta ei löydy haavoittuvuuksia kyseiselle laitteelle. Laitteessa on kuitenkin jotain erittäin mielenkiintoista: se hyödyntää radioviestinnässään rullakoodia (eng. rolling code). Kyseessä on siis tapa estää esimerkiksi signaalin kaappaaminen ja sen lähettäminen uudelleen. Tällä tavoin voitaisiin

avata autotallin ovi yksinkertaisesti toistamalla avaussignaali uudelleen, joka on aivan triviaalitason hyökkäys.

Tätä voisi äkkiseltään pitää hyvänä asiana, sillä laite vaikuttaa nyt hyvin suojatulta. Tarkemmalla tutkimuksella selviää kuitenkin, että laitteiston koko rullakoodijärjestelmä on onnistuttu murtamaan ja siitä on julkaistu koodi, jonka avulla voidaan purkaa vastaanotettua signaalia, sekä lähettää oikeanlaista rullakoodisignaalia puretun signaalin perusteella (Github s.a).

Sekundääriaineiston lisätutkinnan avulla löytyykin blogipostaus, jossa tätä koodia on hyödynnetty autotallin oven avaamiseen. Blogissa kerrotaan, että yksinkertaisella Python-koodilla on onnistuttu purkamaan vastaanotettuja paketteja, joiden avulla saadaan pysyvät sekä rullakoodit. Näitä voidaan käyttää myöhemmin lähettämiseen, eli käytännössä autotallin oven avaamiseen. (Vigue 2022). Tämä on hyvä käytännön esimerkki siitä, että kyseessä ei ole vain pelkkä teoreettinen uhka laitteen turvallisuudelle.

Autotallin oven voi siis avata käytännössä kuka tahansa tarpeeksi aiheeseen perehtynyt henkilö. Lisäksi autotallin käyttäjät voivat olla siinä uskossa, että kyseessä on turvallinen laite, joka voi lisätä ongelman vakavuutta. Onhan laite nimeltään: ”Secplus” eli vapaasti käännettynä: ”Turvaplus”. Tämä ei kuitenkaan ilmiselvästi pidä paikkansa. Lisäksi laitteen sijoituksella voi olla merkitystä kokonaisturvallisuuden kannalta. Tästä syystä laitteen sijaintia lähdettiin tutkimaan tarkemmin paikan päälle. Laitteen löytöpaikan alueelta löytyi kaksi mahdollista autotallin ovea (kuva 45 ja kuva 46).

Kuva 45. Ensimmäinen mahdollinen autotallin ovi

Kuva 46. Toinen mahdollinen autotallin ovi

Ensimmäinen ovi on suuren hotelliketjun parkkihallin ovi. Kuvasta voidaan huomata, että parkkihalliin mahtuu jopa rekka-auto, eli parkkihallia käytetään todennäköisesti tavaran lastaamiseen. On hyvinkin mahdollista, että rikolliset voisivat käyttää tätä heikkoutta hyväkseen. Autotallin avaamisesta ei jäisi myöskään minkäänlaisia fyysisiä jälkiä, joka voisi vaikuttaa mahdollisen rikostutkinnan forensista tutkimusta.

Toinen ovi näyttää olevan rakennuksen asukkaiden käyttämä parkkihallin ovi. Tähän pätee samat riskit kuin aikasempaan oveen, eli rikollisten olisi helppo hyödyntää tätä samaa heikkoutta. Rikolliset voisivat alkaa käyttämään parkkihallia esimerkiksi varastettujen ajoneuvojen säilyttämiseen. Tällöin rikollisista ei jäisi paperijälkeä mihinkään, sillä heidän ei tarvitsisi esimerkiksi vuokrata tilaa ajoneuvojen säilyttämiseen omalla nimellään. Lisäksi parkkihalleissa saatetaan säilyttää esimerkiksi kalliita moottoripyöriä, jotka voitaisiin vain yksinkertaisesti lastata minuuteissa rikollisten pakettiauton kyytiin.

6 TULOKSET

Yhteenvetona tuloksista voidaan sanoa, että laitteita on hyvin paljon erilaisiin käyttötarkoituksiin. Suuri osa laitteista on lähes merkityksettömiä turvallisuuden kannalta, mutta laitteet, jotka liittyvät vähänkään kriittiseen infrastruktuuriin ovat liian usein alttiina jopa naurettavan helpoille hyökkäyksille, kuten yksinkertaisesti signaalin uudelleen toistamiselle. Laitteiden haavoittuvuuksien mitigointiyrityksetkin ovat usein lähinnä ”purukumivirityksiä”, joilla yritetään vain antaa käyttäjälle mielikuva siitä, että laitteen turvallisuudelle on tehty jotakin.

Käsitellyistä laitteista löytyi vain harvoin CVE-tietokannan tuloksia, eli tunnettuja haavoittuvuuksia. Tätä voisi äkkiseltään luulla hyväksi, sillä tunnettuja haavoittuvuuksia ei ole. Tarkemman analyysin jälkeen huomattiin kuitenkin, että pelkästään valmistajan sivustoja tutkimalla voidaan jo kehitellä erilaisia mahdollisia uhkia.

Teoreettisten uhkien lisäksi löytyi myös paljon konkreettisia todisteita siitä, miten eri tasoiset uhat ovatkin usein todistettu toimiviksi myös reaalimaailman tilanteissa. Osa vakavista uhkista on siis todistettu oikeiksi ja kyseessä oleville uhkille alttiina olevat laitteet ovat tälläkin hetkellä käytössä Kotkansaaressa. Tutkimuksen tuloksia voidaan lisäksi yleistää muihin samankaltaisiin alueisiin, koska ei ole erityisiä syitä sille, miksi muut alueet poikkeaisivat merkittävästi Kotkansaaren tuloksista.

Tutkimuskysymykset olivat seuraavat:

1. Voidaanko IoT-laitteiden dataa kerätä tutkimuksessa käytetyllä laitteistolla Wardriving-tekniikkaa hyödyntäen?

2. Miten erilaisten Bluetooth-teknologian datapakettien ja ISM-radiotaajuuksilla toimivien pakettien sisältö vaihtelee ja miten ne voivat tukea tutkimusta?

3. Miten tutkimuksen tuloksia voidaan käyttää kyberturvallisuuden kehittämiseen?

Ensimmäiseen kysymykseen voidaan tutkimuksen tulosten perusteella vastata yksinkertaisesti, että IoT-laitteiden dataa voidaan kerätä tutkimuksessa käytetyllä laitteistolla Wardriving-tekniikkaa hyödyntäen. Tämä voidaan todeta siksi, että primääriaineiston keruu onnistui tällä tavoin.

Toiseen kysymykseen voidaan vastata sillä, että molempien tiedonsiirtotapojen viestintä on yksinkertaista ja ennalta arvattavaa. Tämä koskee erityisesti radiotaajuudella 433.92 MHz toimivia yksinkertaisia sensoreita ja muita laitteita.

Suurin ero näissä teknologioissa on se, että Bluetooth vaatii erillistä yhdistämistä, jossa luodaan turvallinen yhteys. Tämä vaikeuttaa esimerkiksi man in the middle -hyökkäyksen suorittamista, mutta ei kuitenkaan estä sitä täysin. Yksinkertaiset radiolaitteet taas hyväksyvät lähes minkä tahansa vastaanottamansa signaalin, joka käyttää samoja yksinkertaisia viestintätapoja. Tämä tekee yksinkertaisista radiolaitteista alttiimpia helpoille hyökkäyksille. Bluetooth-teknologiaan kohdistuvat hyökkäykset vaativat hieman enemmän aikaa, vaivaa ja osaamista.

Tutkimusta tukivat paketit, jotka sisältivät mielenkiintoisia lisätietoja laitteesta. Esimerkiksi autojen rengaspainemittarit paljastivat tiedoillaan sen, onko autolla ajettu lähiaikoina. Tämä auttoi tutkimuksen riskianalyysissä ja mahdollisten väärinkäyttökohteiden spekuloinnnissa. Lisäksi moni laite kertoi suoraan laitteen tarkan mallin ja muita tietoja, joita ei olisi välttämättä tarpeellista mainostaa. Tämä seikka mahdollisti merkittävästi tutkimuksen toteuttamista.

Kolmanteen kysymykseen voidaan vastata niin, että tutkimuksen tuloksia voidaan hyödyntää kyberturvallisuuden kehittämisessä monin tavoin. Tulokset paljastavat aikaisemmin piilossa olleita ongelmia, jotka voidaan ottaa huomioon jatkossa, kun kehitetään esimerkiksi kaupungin infrastruktuuria. Lisäksi tulokset tarjoavat syvää ymmärrystä riskitekijöistä ja niiden taustalla olevista tekijöistä. Tämä auttaa muun muassa kehittämään yhä turvallisempia laitteita.

Tutkimustuloksia voidaan käyttää myös koulutuksessa sekä tietoisuuskampanjoissa, joiden avulla voidaan lisätä yleistä ymmärrystä IoT-laitteista. Lisäksi tulokset voivat tuoda hyödyllistä tietoa tietoturvayhteisöille ja viranomaisille. Tämä voi parantaa merkittävästi yleistä kyberturvallisuuden tasoa.

7 JOHTOPÄÄTÖKSET

Tutkimusongelmana oli se, että IoT-laitteiden kyberturvallisuustilannetta ei olla kartoitettu tarpeeksi kaikkien tiedonsiirtoteknologioiden osalta. Tutkimuksessa tutkittiin näitä vähemmälle jääneitä tiedonsiirtoteknologioita ja tutkimuksen avulla saatiin analysoitujen tulosten lisäksi tarkempaa dataa, jota voidaan käyttää vieläkin laajempaan kartoittamiseen. Kotkansaaren IoT-laitteiden kyberturvallisuustilannetta on nyt siis kartoitettu kattavasti useamman tiedonsiirtoteknologian osalta. Tästä syystä voidaan sanoa, että tutkimusongelmaan on saatu ratkaisu.

8 POHDINTA

Kokonaisuudessaan voidaan todeta, että monen IoT-laitteen kyberturvallisuuden taso on huono. Näiden heikosti suojattujen laitteiden ongelmat koskevat meidän kaikkien turvallisuutta. Tämä koskee erityisesti Wardrivingin avulla löytyneitä laitteita, sillä mikään ei estä myös muita henkilöitä löytämästä näitä samoja laitteita.

Syy tähän huonoon kyberturvallisuuden tasoon voi olla se, että aihetta on tutkittu suhteellisen vähän verrattuna esimerkiksi Wi-Fi-verkkojen kartoittamiseen. Esimerkiksi internettiin liittyyvät haavoittuvuudet, kuten API-sovellusohjelmointirajapintaan liittyvät haavoittuvuudet löydetään yleensä nopeasti. Samaa ei voisi sanoa haavoittuvuuksista, jotka vaativat ohjelmistoradion käytön.

Tämä johtuu todennäköisesti siitä, että ohjelmistoradio-osaaminen on harvinaisempaa kuin verkkoprotokollien osaaminen. Juuri tästä syystä asiaa on tärkeä tuoda ilmi. Tämän avulla voidaan kehittää parempia ratkaisuja laitteiden suojaamiseksi ja löytää vahvoja perusteita yleisen osaamistason parantamiseksi myös ohjelmistoradio-osaamisen osalta.

8.1 Työn onnistuminen

Primääriaineiston keruussa törmättiin joihinkin ongelmiin, jotka vaikuttavat osittain tutkimuksen tuloksiin. Näistä ongelmista kertominen on tärkeää, sillä ongelmien ilmi tuominen tekee tutkimuksesta luotettavamman ja helpommin ymmärrettävän. Tämä estää vääränlaisten tulkintojen syntymisen tuloksista. Tutkimuksen tulokset tuovat tärkeää tietoa ja tuloksia voidaan hyödyntää kyberturvallisuuden parantamisessa. Tutkimus toteutettiin tavalla, joka maksimoi hyödyt ja minimoi mahdolliset haitat.

Ensimmäinen havaittu ongelma löytyi siitä, että taajuuksia 315 MHz ja 915 MHz käyttävien RTL-SDR-vastaanottimien antennit poikkeavat hieman näistä taajuuksista. Tämä ei kokonaan estä radiosignaalien vastaanottamista, mutta tämä on hyvä ottaa huomioon esimerkiksi laitteiden lukumääriä tutkiessa.

Toinen havaittu ongelma oli se, että Kotkamillsin alueelle ei päästy suorittamaan Wardrivingia ollenkaan. Tämä johtui siitä, että aluelle ei päässyt liikkumaan laillisin keinoin. Tämän mainitseminen on merkittävää, sillä alue oli yksi kiinnostavaksi määritellyistä kohteista. Lisäksi Kotkamillsin alue kattaa merkittävän osan koko Kotkansaaren pinta-alasta, mikä tarkoittaa sitä, että yksi iso osa Kotkansaaren kartoittamisesta puuttuu kokonaan.

Kolmas havaittu ongelma löytyi siitä, että Wardrivingissa käytetty ohjelmisto ei tue läheskään kaikkia IoT-laitteita. Kismet käyttää lähteenä ohjelmistoa nimeltä: ”RTL_433”. Kyseisen ohjelmiston toiminta perustuu vahvasti siihen, että ihmiset ovat vapaaehtoisesti lisänneet tunnistettavia laitteita ohjelmaan. Tämä koskee pelkästään yksinkertaisia ISM-radiotaajuuksia käyttäviä laitteita eikä esimerkiksi Bluetooth-laitteita. Tämä tarkoittaa sitä, että tutkimuksen tuloksia ei voida pitää kaiken kattavana kartoituksena.

Neljäs havaittu ongelma oli se, että henkilöautolla ajaminen saattoi estää joidenkin laitteiden löytymisen kokonaan. Antennit asetettiin auton kojelaudalle, jotta auton metallinen kori ei estäisi merkittävästi radiosignaalien vastaanottamista. Parempia tuloksia olisi kuitenkin voitu saada asettamalla antennit esimerkiksi auton katolle. Tämä oli kuitenkin haastava toteuttaa sääolosuhteiden ja antennityyppien takia, joten tutkimuksessa tyydyttiin

hieman heikompaan ratkaisuun. Tämä ei kuitenkaan välttämättä tarkoita, että tutkimustulokset olisivat joka tapauksessa olleet merkittävästi erilaisia, sillä radiosignaalit kulkevat kuitenkin suhteellisen hyvin myös joidenkin fyysisten esteiden läpi.

Viidentenä ongelmana havaittiin se, että ajonopeudella on todennäköisesti merkitystä löytyneiden laitteiden määrään. Ajaminen toteutettiin vaihtelevin nopeuksin. Keskimääräinen nopeus oli arviolta noin 20 km/h luokkaa. Ajonopeuden muutokset saattavat vaikuttaa merkittävästi löydettyjen laitteiden määrään, sillä osa laitteista saattaa lähettää dataa vain harvoin.

Kokonaisuudessaan edellä mainitut ongelmat eivät todennäköisesti vaikuta merkittävästi tutkimuksen tuloksiin (pois lukien toisena lueteltu aihe). Tämä johtuu pääasiassa siitä, että tutkimuksen ei ollut alun perinkään määrä olla absoluuttinen ja kaiken kattava kartoitus. Tulokset riittävät antamaan uutta ja tärkeää tietoa tarpeeksi hyvällä tarkkuudella. Liian tarkka pureutuminen yksittäisiin seikkoihin olisi myös todennäköisesti estänyt lopulta koko tutkimuksen suorittamisen jo pelkästään ajallisten rajoitteiden vuoksi.

8.2 Luotettavuus

Tutkimus tehtiin avoimesti ja noudattaen lakia sekä aikaisemmin määriteltyjä eettisiä sääntöjä. Tutkimuksessa käytetyt tavat voidaan tarpeen tullen toistaa, jolloin tulosten voidaan katsoa olevan läpinäkyviä. Lisäksi mahdolliset ongelmat on tuotu esille selkeästi, sekä tulokset ollaan analysoitu objektiivisesti pohjaten kattavaan sekundääriaineistoon.

Tutkimuksessa käytetty laitteisto on suhteellisen halpaa ja kaikki tutkimuksen aikana kerätty data pidetään tallessa mahdollisimman pitkään. Tutkimuksen dataa voidaan jakaa muille tarkasteltavaksi, jotta sen eheys ja tutkimuksen luotettavuus voidaan todeta. Tätä rajoittaa kuitenkin tutkimuksessa aikaisemmin määritellyt eettiset säännöt ja yksityisyys.

Tutkimuksessa käytetyn laitteiston halpa hinta mahdollistaa tutkimuksen toistamisen, vaikka siihen ei olisi saatavilla suurta budjettia. Tällaiset

tutkimustavat vahvistavat tutkimuksen luotettavuutta ja antavat pohjan jatkotutkimuksille sekä muunlaiselle tulosten hyödyntämiselle.

8.3 Jatkokehitys

Jatkokehityksenä tutkimuksen mukaista Wardrivingia voitaisiin suorittaa Kotkansaaren lisäksi myös muilla alueilla. Alue voisi keskittyä esimerkiksi pelkästään jonkin kriittisen kohteen alueelle. Tämä voisi olla esimerkiksi nyt tutkimuksesta pois jäänyt Kotkamillsin alue. Alueen IoT-laitteita voisi kartoittaa kävelemällä alueella tai ajamalla erittäin hitaasti. Tämä voisi tuoda tarkempia tuloksia yhden alueen suhteen.

Wardrivingia voitaisiin käyttää myös tiettyjen alueiden turvallisuuden ylläpitämiseen. Säännölliset kartoitukset mahdollistaisivat esimerkiksi sen, että tietyiltä alueilta voitaisiin yksinkertaisesti poistaa kyberturvallisuudelle haitalliset laitteet. Näitä voisi olla esimerkiksi armeijan alueet tai esimerkiksi sairaaloiden alueet, joissa turvallisuus on erityisen tärkeää.

Wardriving-kartoitusta olisi mahdollista suorittaa myös esimeriksi drooneilla lentäen. Tämä mahdollistaisi haastavien paikkojen tiedustelun. Esimerkiksi maanpuolustustilanteessa drooneilla voitaisiin lentää etukäteen alueelle, jossa epäillään olevan erilaisia laitteita. Laitteista voidaan sitten tehdä tutkimusta ja tällä tavoin voidaan kehittää erilaisia jatkosuunnitelmia puolustuksen suhteen.

Lisäksi Wardrivingia voitaisiin hyödyntää tilastotietojen keräämisessä. Esimerkiksi jokin yritys saattaisi olla kiinnostunut selvittämään, kuinka monta heidän valmistamaansa laitetta käytetään tietyllä alueella. Tätä tietoa voitaisiin käyttää myöhemmin esimerkiksi markkinoinnissa tai muussa kehityksessä.

Yhteenvetona Wardrivingin tutkimuksen tuomat jatkokehitysmahdollisuudet ovat lähes rajattomat. Kaiken rajana on oikeastaan vain mielikuvitus ja tutkijan taidot. Tämä tarkoittaa sitä, että Wardriving on potentiaalinen työkalu monenlaisille sovelluksille ja tutkimuksille, jotka liittyvät IoT-laitteiden turvallisuuteen, paikannukseen, tai datan keräämiseen ja analysointiin erilaisissa ympäristöissä.

LÄHTEET

About RTL-SDR. RTL-SDR s.a. WWW-dokumentti. Saatavissa: https://www.rtl-sdr.com/about-rtl-sdr/ [viitattu 6.2.2024].

Airbreak.dev. Jailbreak your CPAP machine with Airbreak. 2020. WWW-dokumentti. Päivitetty 15.4.2024. Saatavissa: https://airbreak.dev/ [viitattu 11.3.2024].

AlMarzouq, M., Zheng, L., Rong, G., & Grover, V. 2005. Open source: Concepts, benefits, and challenges. PDF-dokumentti. Saatavissa: https://www.researchgate.net/profile/Mohammad-Almarzouq-3/publication/288520793_Open_Source_Concepts_Benefits_and_Challenges/links/6426d24da1b72772e43ed1d3/Open-Source-Concepts-Benefits-and-Challenges.pdf [viitattu 9.2.2024].

Clifford, J. 2022. Tyre pressure warning light: What is it?. WWW-dokumentti. Päivitetty 14.12.2022. Saatavissa: https://mag.toyota.co.uk/how-does-tpms-work/ [viitattu 8.2.2024].

Daveking Wiki 2021. Use Android Phone As GPS With Kismet. WWW-dokumentti. Päivitetty 16.1.2021. Saatavissa: https://wiki.daveking.com/index.php?title=Use_Android_Phone_As_GPS_With_Kismet [viitattu 11.2.2024].

Day, L. 2022. Ev chargers could be a serious target for hackers. WWW-dokumentti. Päivitetty 28.11.2022. Saatavissa: https://hackaday.com/2022/11/28/ev-chargers-could-be-a-serious-target-for-hackers/ [viitattu 28.2.2024].

Debian käyttöohjeet s.a. Rtl_test. WWW-dokumentti. Päivitetty 25.8.2023. Saatavissa: https://manpages.debian.org/testing/rtl-sdr/rtl_test.1.en.html [viitattu 23.2.2024].

Decuir, J. 2010. Bluetooth 4.0: Low Energy. PDF-dokumentti. Saatavissa: https://www.ineltek.com/wp-content/uploads/2015/09/20160330-IEEE_BLE.pdf [viitattu 9.2.2024].

Exploring vulnerabilities in tire pressure monitoring systems tpms with a HackRF. 2017. RTL-SDR. WWW-dokumentti. Päivitetty 30.11.2024. Saatavissa: https://www.rtl-sdr.com/exploring-vulnerabilities-in-tire-pressure-monitoring-systems-tpms-with-a-hackrf/ [viitattu 30.2.2024].

Fortinet s.a. What is Wardriving? WWW-dokumentti. Saatavissa: https://www.fortinet.com/resources/cyberglossary/wardriving [viitattu 9.2.2024].

Fürst, J., Chen, K., Kim, H. S., & Bonnet, P. 2018. Evaluating Bluetooth low energy for IoT. PDF-dokumentti. Päivitetty 2018. Saatavissa: https://pure.itu.dk/ws/files/83650621/cps_bench_final.pdf [viitattu 6.2.2024].

Garage_door-opener-1024x633.jpg. 2017. WWW-kuvatiedosto. Saatavissa: https://automaticgaragesolutions.com.au/wp-content/uploads/2017/09/1200px-Garage_door_opener-1024x633.jpg [viitattu 12.3.2024].

Georgakakis, E., Nikolidakis, S. A., Vergados, D. D., & Douligeris, C. 2011. An analysis of bluetooth, zigbee and bluetooth low energy and their use in wbans. PDF-dokumentti. Saatavissa: https://eudl.eu/pdf/10.1007/978-3-642-20865-2_22 [viitattu 9.2.2024].

Gerring, J. 2004. What Is a Case Study and What Is It Good for? PDF-dokumentti. Saatavissa: https://indiachinainstitute.org/wp-content/uploads/2017/05/4B-What-Is-A-Case-Study-Gerring-2004.pdf [viitattu 10.2.2024].

Github s.a. Rtl_433. WWW-dokumentti. Päivitetty 11.2.2024. Saatavissa: https://github.com/merbanan/rtl_433/blob/master/README.md [viitattu 11.2.2024].

Github s.a. Secplus. WWW-dokumentti. Saatavissa: https://github.com/argilo/secplus [viitattu 12.3.2024].

Google 2022. Google Earth. WWW-dokumentti. Päivitetty 2022. Saatavissa https://earth.google.com/ [viitattu 12.3.2024].

HackerOne s.a. Hackerone.com. WWW-dokumentti. Saatavissa: https://hackerone.com/resmed [viitattu 11.3.2024].

Idesco s.a. Idesco.fi. WWW-dokumentti. Saatavissa: https://idesco.fi/ [viitattu 20.2.2024].

Intro to OpenStreetMap. s.a. mattcen.github.io. WWW-kuvatiedosto. Saatavissa: https://mattcen.github.io/intro-to-openstreetmap/ [viitattu 2.2.2024].

Kail, E., Banati, A., László, E., & Kozlovszky, M. 2018. Security survey of dedicated IoT networks in the unlicensed ISM bands. PDF-dokumentti. Päivitetty 05.2018. Saatavissa: https://www.researchgate.net/profile/Anna-Banati/publication/327194882_Security_Survey_of_Dedicated_IoT_Networks_in_the_Unlicensed_ISM_Bands/links/5f0d53ce4585155a552823c9/Security-Survey-of-Dedicated-IoT-Networks-in-the-Unlicensed-ISM-Bands.pdf [viitattu 5.2.2024].

Kaspersky s.a. What is jailbreaking? WWW-dokumentti. Saatavissa: https://www.kaspersky.com/resource-center/definitions/what-is-jailbreaking [viitattu 12.3.2024].

Kiinteistön kulunvalvonta uudelle turvatasolle Seos-teknologian avulla. 2017. Hedengren. WWW-dokumentti. Päivitetty 31.10.2017. Saatavissa: https://www.hedengren.com/fi/kiinteiston-kulunvalvonta-uudelle-turvatasolle-seos-teknologian-avulla [viitattu 20.2.2024].

Kismet s.a. Kismet. WWW-dokumentti. Saatavissa: https://www.kismetwireless.net/ [viitattu 11.2.2024].

Laadullinen tutkimus. 2015. Koppa. WWW-dokumentti. Päivitetty 28.10.2021. Saatavissa: https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/laadullinen-tutkimus [viitattu 11.2.2024].

Latausasema EVC-04 – Vestel EVC-04 7.4kW – Vestel / Finlux Pro. 2021. Finluxpro. PDF-dokumentti. Päivitetty 11.01.2021. Saatavissa: https://finluxpro.com/wp-content/uploads/2021/01/Snro_3418900_20210111.pdf [viitattu 28.2.2024].

Learn About Bluetooth. s.a. Bluetooth Technology Overview. WWW-dokumentti. Saatavissa: https://www.bluetooth.com/learn-about-bluetooth/tech-overview/ [viitattu 7.2.2024].

Lee, I. 2020. Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. PDF-dokumentti. Saatavissa: https://www.mdpi.com/1999-5903/12/9/157/pdf [viitattu 9.2.2024].

Lähdesmäki, T., Hurme, P., Koskimaa, R., Mikkola, L. & Himberg, T. 2009. Jyväskylän yliopisto. Saatavissa:

https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/aineiston-analyysimenetelmat [viitattu 9.2.2024].

Madakam, S. , Ramaswamy, R. And Tripathi, S. 2015. Internet of Things (IoT): A Literature Review. WWW-dokumentti. Saatavissa: https://www.scirp.org/html/56616_56616.htm [viitattu 8.2.2024].

Massie, G. 2022. Russian EV charging stations hacked with ‘Putin is a d***head’ message. WWW-dokumentti. Saatavissa: https://www.independent.co.uk/news/world/europe/putin-charging-station-hacked-ukraine-russia-b2026260.html [viitattu 8.2.2024].

Mikä on henkilötieto? s.a. Tietosuojavaltuutetun toimisto. WWW-dokumentti. Saatavissa: https://tietosuoja.fi/mika-on-henkilotieto [viitattu 11.2.2024].

Mitre 2023. Mitre.org. WWW-dokumentti. Päivitetty 14.8.2023. Saatavissa: https://cve.mitre.org/ [viitattu 12.3.2024].

Onninen s.a. KÄYTTÖVESIPUMPPU WILO STRATOS MAXO-Z 25/0,5-8 180mm. WWW-dokumentti. Saatavissa: https://www.onninen.fi/wilo-kayttovesipumppu-wilo-stratos-maxo-z-25-0-5-8-180mm/p/CHN903 [viitattu 20.2.2024].

Osmocom 2016. Rtl-sdr. WWW-dokumentti. Päivitetty 25.7.2022. Saatavissa: https://osmocom.org/projects/rtl-sdr/wiki/Rtl-sdr/ [viitattu 8.2.2024].

Pseudonymisoidut ja anonymisoidut tiedot. s.a. Tietosuojavaltuutetun toimisto. WWW-dokumentti. Saatavissa: https://tietosuoja.fi/pseudonymisointi-anonymisointi [viitattu 2.11.2024].

Radiolaki 16.11.2001/1015.

Radiotaajuusmääräys 4AE2024M.

ResMed s.a. ResMed.fi. WWW-dokumentti. Saatavissa: https://www.resmed.fi [viitattu 11.3.2024].

Shaked, Y., & Wool, A. 2005. Cracking the bluetooth pin. PDF-dokumentti. Saatavissa: https://www.usenix.org/legacy/event/mobisys05/tech/full_papers/shaked/shaked.pdf [viitattu 20.2.2024].

Signify s.a. Signify.fi. WWW-dokumentti. Saatavissa: https://www.signify.com/fi-fi [viitattu 30.2.2024].

Soumyalatha, Shruti G. Hegde. 2016. Study of IoT: understanding IoT architecture, applications, issues and challenges. PDF-dokumentti. Saatavissa: https://www.researchgate.net/profile/Soumyalatha-Naveen/publication/330501274_Study_of_IoT_Understanding_IoT_Architecture_Applications_Issues_and_Challenges/links/5c434fea458515a4c731d4bb/Study-of-IoT-Understanding-IoT-Architecture-Applications-Issues-and [viitattu 8.2.2024].

Stillianopoulus, N. 2022. Russian Charging Stations Hacked To Display 'Putin Is A Dickhead' Message. WWW-dokumentti. Päivitetty 4.3.2024. Saatavissa: https://www.thinkinghumanity.com/2022/03/russian-charging-stations-hacked-to-display-putin-is-dickhead-message.html [viitattu 8.2.2024].

Vigue, A. 2022. Garage Door Hacking. WWW-dokumentti. Päivitetty 6.5.2022. Saatavissa: https://vigue.me/posts/hacking-security-2-0 [viitattu 12.3.2024].

Wilo 2022. Wilo-Smart Connect Module BT. PDF-dokumentti. Päivitetty 3.4.2022. Saatavissa: https://cms.media.wilo.com/dcidocpfinder/wilo511087/5900207/wilo511087.pdf [viitattu 21.2.2024].

WiGLe.net 2024. All the networks. Found by Everyone. WWW-dokumentti. Saatavissa: https://wigle.net [viitattu 8.2.2024].

Zuazola, I. G., Sharma, A., Batchelor, J. C., Angulo, I., Perallos, A., Whittow, W. G., ... & Langley, R. 2012. Radio frequency Identification miniature interrogator antenna sprayed over an in-vehicle chassis. PDF-dokumentti. Saatavissa: https://research.mobility.deustotech.eu/media/publications/2012/journalarticle/radio-frequency-identification-miniature-interrogator-antenna-sprayed-over-an-in-vehicle-chassis.pdf [viitattu 11.2.2024].