Älykodin kyberturvallisuus

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulun opinnäytetyö

Tietojenkäsittelyn koulutusohjelma

Hämeenlinnan korkeakoulukeskus, kevät 2020

Timo Myllylä

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Hämeenlinna
Tietojenkäsittelyn koulutusohjelma

Tekijä Timo Myllylä **Vuosi** 2020

Työn nimi Älykodin kyberturvallisuus

Työn ohjaaja Lasse Seppänen

TIIVISTELMÄ

Tässä opinnäytetyössä tutkittiin älykodin kyberturvallisuutta ja keinoja parantaa sitä. Tarkoituksena oli selvittää, onko mahdollista tehdä käytettävyydeltään hyvä ja turvallinen älykoti niin, että käyttäjä säilyttää kontrollin omaan dataansa ja että yksityisyys on turvattu. Älykodin toiminnallisuus jätettiin tässä opinnäytetyössä tarkastelun ulkopuolelle.

Toteutusvaiheessa rakennettiin testiympäristö, jota tutkittiin ja johon otettiin etäyhteyksiä. Testiympäristön lisäksi tutkittiin älykodin käyttöön soveltuvia langattomia tiedonsiirtotekniikoita ja älykodin kyberturvallisuuteen vaikuttavia asioita. Testiympäristö koostui Ikean Trådfri-sarjan laitteista, Raspberry PI -korttitietokoneesta ja Home Assistant -älykotisovelluksesta. Tehtyyn testiympäristöön muodostettiin etäyhteys TOR-verkon kautta. Opinnäytetyössä kuvataan helppokäyttöisen älykodin ja etäyhteyden asennus, minkä lisäksi annetaan suosituksia älykodin rakentajalle.

Lopputuloksena onnistuttiin tekemään avoimiin ja vapaasti käytettävissä oleviin ohjelmistoihin pohjautuva älykoti, jossa käyttäjällä on mahdollisuus kontrolloida omaa datansa ja yksityisyyttä. Löydettiin myös helppo ja monipuolinen älykotisovellus, jota voi käyttää eri ympäristöissä ja erilaisten laitteiden kanssa. Langattomien tiedonsiirtotekniikoiden ominaisuuksia ja eroavaisuuksia älykotikäytössä vertailtiin. Älykodin rakentamista varten löytyi paljon kyberturvallisuuteen liittyviä ehdotuksia ja suosituksia. Jatkotutkimuksena voisi selvittää syvällisesti langatonta tiedonsiirtoa ja sen kybertuvallisuutta.

Avainsanat kyberturvallisuus, älykoti, langaton tiedonsiirto, Home Assistant, TOR

Sivut 36 kpl

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Hämeenlinna
Degree Programme in Business Information Technology

Author Timo Myllylä **Year** 2020

Subject of Bachelor's thesis Cyber Security of the Smart Home

Supervisor Lasse Seppänen

ABSTRACT

This thesis explores the cyber security of smart homes and ways to improve it. The purpose was to find out whether it is possible to make a smart home that is usable and secure, while the user maintains control over his own data and privacy. The functionality of the smart home was excluded from this thesis.

A test environment was built for research and testing. Wireless communication technologies for smart homes and cyber security issues were also studied. The test environment consisted of Ikea's Trådfri devices, the Raspberry PI card computer and the Home Assistant smart home application. A remote connection to the test environment was created via the TOR network. The thesis describes the installation of an easy-to-use smart home and remote connection, as well as recommendations for the smart home user.

The result of this thesis was a smart home setup that is based on open and freely available software. In this setup the user has control over his own data and privacy. Home Assistant was an easy and versatile smart home application that can be used in different environments and devices. The features and differences of wireless communication technologies for smart home use were compared. Many suggestions and recommendations on cyber security were found for a smart home user. There is a need for further research on wireless data transfer technologies and cyber security.

Keywords cyber security, smart home, wireless communication, Home Assistant, TOR.

Pages 36 p.

SANASTO

IoT	Internet of Things
IoE	Internet of Everything
LPWAN	Low Power Wide Area Network
DNS	Domain Name System
DHCP	Dynamic Host Configuration Protocol
MAC	Media Access Control
NAT	Network Address translation
MESH	Mesh Networking

Seuraavat termit määritelmineen on otettu Sanastokeskuksen sanastosta (Sanastokeskus TSK ry, 2020):

palomuuri; suojamuuri

tekninen järjestely, jonka on tarkoitus estää asiaton pääsy verkosta toiseen

reititin — laite tai ohjelmisto, joka ohjaa tietoliikennettä sopivalle reitille kohti määränpäätä

Tor-verkko — tietoverkko, jossa internetliikenne kiertää salattuna useiden ympäri maailmaa vapaaehtoistyöllä ylläpidettyjen palvelimien kautta.

internet; Internet; netti

maailmanlaajuinen avoin tietoverkko, joka ytimeltään perustuu TCP/IP-yhteyskäytäntöjen käyttöön

IP-osoite; IP-numero

Internetiin kytketyn tietojenkäsittely- tai tiedonsiirtolaitteen tai verkkoliittymän yksilöivä numeerinen tunnus

kybertoimintaympäristö

yhdestä tai useammasta digitaalisesta tietojärjestelmästä muodostuva toimintaympäristö

kyberturvallisuus

tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan

kyberuhka

mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku, joka kohdistuu kybertoimintaympäristöön ja toteutuessaan vaarantaa siitä riippuvaisen toiminnon

tietoturva; tietoturvallisuus

järjestelyt, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus

haavoittuvuus

alttius tietoturvaan kohdistuville uhkille

monivaiheinen todentaminen

todentaminen vähintään kahta eri menetelmää käyttäen

SISÄLLYS

1 JOHDANTO JA TAVOITTEET

Ihmiset etsivät yhä enemmän ratkaisuja kodin arjen helpottamiseksi. Älykoti eri ominaisuuksineen on alkanut kiinnostaa kuluttajia, ja markkinoille on tullut paljon älykotituotteita. Älykotituotteita ja muita älykkäiksi markkinoituja tuotteita on saatavilla useimmista marketeista ja kodinkoneliikkeistä, joten tuotteiden ostaminen on vaivatonta. Vaikka tuotteet yksinään ovat helppokäyttöisiä, niiden käyttämät tekniikat ja toteutustavat kuitenkin vaihtelevat suuresti. Sen vuoksi älykodin rankentajan on oletettavasti vaikeaa ymmärtää ja hallita älykotia kokonaisuutena. Epävarmuus luo pelkoja kyberturvallisuudesta ja yksityisyyden suojasta, joten kuluttaja saattaa jättää tekemättä älykotiin liittyviä hankintoja.

Älykotiin ja älykodin tekniikkaan liittyviä tutkimuksia ja opinnäytetöitä on tehty useita. Niissä on käsitelty pääasiassa yksittäisiä teknologioita, mutta niissä ei ole usein ollut tarkoituksena tutkia älykotia kokonaisuutena eikä käyttäjän näkökulmasta.

Tämän opinnäytetyön tavoitteena on tutkia älykodin kyberturvallisuutta ja löytää ratkaisuja käytettävyydeltään hyvän ja kyberturvallisen älykodin toteuttamiseksi. Älykodissa käytetään paljon langatonta tiedonsiirtoa, johon on tarjolla useita teknologioita. Opinnäytetyössä selvitetään langattomien tiedonsiirtotekniikoiden eroja ja niiden soveltuvuutta älykodin rakentamiseen. Älykodin toiminnallisuutta ja säätömahdollisuuksia ei tässä opinnäytetyössä tutkita. Tekniikoista pyritään tuomaan esille sellaisia asioita, joista on älykodin rakentajalle käytännön hyötyä. Tekniikoiden tarkkoja yksityiskohtia ei siten käsitellä tässä opinnäytetyössä.

Testiympäristöksi rakennettiin sellainen yksinkertainen älykoti, jonka tavallinen älykodin rakentaja voi helposti tehdä markkinoilla saatavilla olevista komponenteista. Testiympäristöllä tutkittiin älykodin kybertuvallisuutta ja testattiin tapoja toteuttaa älykodin etäyhteyksiä.

Opinnäytetyössä pyritään vastaamaan seuraaviin kysymyksiin: Mitä kyberturvallisuusasioita älykodin rakentajan pitää ottaa huomioon? Miten älykotiin muodostetaan tietoturvallinen etäyhteys? Lisäksi tarkoituksena on luoda suosituksia ja tarkistuslista älykodin rakentajalle.

2 ÄLYKOTI

Megatrendejä selvittävän Sitran julkaisussa nostetaan yhdeksi megatrendiksi tekniikan sulautuminen kaikkeen. Teknologian muutos on osa isompaa yhteiskunnan ja maailman muutosta, johon liittyy esimerkiksi väestön ikääntyminen sekä kysymys siitä, kuka päättää teknologiasta ja datan roolista. (Dufva, 2020, s. 8–9)

Teknologia ja tekoäly tulevat kaikkialle ihmisten arkeen, myös kotiin erilaisina älykotiratkaisuina. Jo nyt on käytössä älykotiratkaisuja, joissa voidaan automatisoida ja ohjata toimintoja erilaisten sensoritietojen avulla. Tulevaisuudessa tekoälyn lisääntyessä saadaan kodeista entistä älykkäämpiä, jolloin ne tekevät jopa itsenäisiä päätöksiä.

Esimerkiksi Åkerblom (2017, s 8) pohtii arkkitehtuurin opinnäytetyössään älyn ja älykkyyden määritelmää ja sitä, onko kaikissa älylaitteiksi mainituissa laitteissa oikeastaan älyä lainkaan. Myös tätä opinnäytetyötä tehtäessä nousi esille pohdinta siitä, että älykotipakettina markkinoidut tuotteet eivät usein ole varsinaisesti älykkäitä. Kun kännykän sovelluksella voi säätää valoja päälle ja pois, on kyse lähinnä vain valaistuksen kauko-ohjauksesta. Sen sijaan älykkyydestä voidaan puhua, kun laite tekee ratkaisuja keräämänsä datan perusteella. Kun laite säätää valaistusta esimerkiksi auringon nousun ja laskun tai säätilan perusteella, voidaan puhua laitteen jonkinasteisesta älykkyydestä.

Älykoti palvelee laadukasta arkea, lisää ilmastoviisautta ja edistää terveyttä (Åkerblom, 2017, s. 28). Esimerkiksi ilmastoinnin ja lämmityksen ohjaaminen keskitetysti mahdollistaa paremman energiatehokuuden ja paremman hengitysilman laadun. Erilaiset automatisoidut toiminnot parantavat asujan arkea, koska ne voivat hoitaa osan kodin töistä. Esimerkkinä voidaan mainita siivouksen tai ruohonleikkuun automaattisesti hoitavat robotit.

Nykyään monet ovat varsin valveutuneita tietoturvan suhteen. On ymmärrettävää, että älykotia suunnittelevia mietityttää, mihin älykodin keräämä tieto päätyy ja mitä sillä tehdään. Älykodin suunnittelussa voi syntyä myös ristiriitaisia ajatuksia. Esimerkiksi kuluttaja voi hakea turvaa vaikkapa valvontajärjestelmän asentamisella, mutta toisaalta hänelle syntyy pelkoja tietomurroista. Älykotilaitteistoja hankkiessaan kuluttaja joutuu punnitsemaan ratkaisun hyötyjä ja uhkia. Keskivertokansalaisella ei kuitenkaan voida olettaa olevan riittävästi tietoa ja osaamista turvallisen älykotiratkaisun tekemiseksi.

Uutisointi erilaisista älykoteihin liittyvistä ongelmista lisää helposti pelkoa yksityisyyden menettämisestä ja herättää kysymyksiä älykodin kyberturvallisuudesta. Esimerkiksi kroatialaisesta Zipaton-älykotijärjestelmästä löydettiin tietoturva-aukko, jonka avulla onnistuttiin saamaan järjestelmän pääkäyttäjän oikeudet (Talouselämä, 2019). Toisessa esimerkkitapauksessa murtauduttiin kodin valvontakameraan ja häiriköitiin perheen elämää (tivi, 2020).

Pelot voivat olla myös älykotitoimittajien kannalta ongelmallisia, koska osa kuluttajista voi jopa jättää epätietoisuuden vuoksi älykotihankinnat kokonaan tekemättä. Siksi on tärkeää, että kuluttaja saa myyjältä riittävästi perustietoa kyberturvallisuudesta sekä vinkkejä lisätietoihin. Suomessa myös Liikenne- ja viestintävirasto Traficom pyrkii lisäämään kuluttajien tietoisuutta kyberturvallisuuteen liittyvistä asioista erilaisin julkaisuin ja kampanjoin. Traficom julkaisi vuoden 2019 lopussa Tietoturvamerkin, joka voidaan myöntää sellaisille kodin älylaitteille, joiden tietoturvan perusominaisuudet ovat kunnossa. (Liikenne- ja viestintävirasto Traficom, 2020)

Edellä mainittujen pelkojen vuoksi älykotiratkaisut voivat vaikuttaa myös teknisesti hankalilta toteuttaa ja ottaa käyttöön. Älykotilaitteiden valmistajat ovat pyrkineet ja usein onnistuneetkin tekemään älykodin laitteista mahdollisimman helppokäyttöisiä. Esimerkiksi Ikea myy älykotiratkaisuja, jossa asennus onnistun kännykän sovelluksen ja kuvallisten ohjeiden avulla. Vaikka yksittäiset laitteet ovat usein helppokäyttöisiä, vaikeuksia ilmenee edelleen eri valmistajien laitteiden yhteensovittamisessa. On vaikeaa löytää yksi laite, jolla voi ohjata kaikkia kodin laitteita.

2.1 Kotiverkon teknologiat ja laitteet

Kotiverkko on kodin tietoliikenneverkko, johon tietokoneita ja muita laitteita voidaan liittää kaapelilla tai langattomalla WiFi-yhteydellä. Kotiverkon kaapelilla toimivaa osuutta kutsutaan LAN-verkoksi ja langatonta verkkoa WLAN-verkoksi. Julkinen verkko puolestaan on kodin ulkopuolinen verkko, johon kodinverkko liitetään reitittimen kautta.

Älykodin rakentajalla on hyvä olla yleiskuva ainakin seuraavista teknologioista ja laitteista: reititin, kotiverkko, palomuuri ja IP-osoite. Näin voi muodostaa käsityksen siitä, miten älykodin kokonaisuus rakentuu ja mitä sen kyberturvallisuuteen liittyy. Kotikäytössä reitittimellä tarkoitetaan yleensä laitetta, jonka kautta saadaan yhteys internetiin. Internetyhteyden lisäksi kodin reititin voi hoitaa myös muut verkon toiminnot.

Yhtenä osana kotiverkon suojaamiseksi käytetään niin sanottuja palomuureja, joilla erotetaan kotiverkko ja julkinen verkko. Yleensä kodin reitittimessä on yhtenä osana palomuuri, ja kodin tietokoneissa on palomuuriohjelma.

Yhden IP-osoitteen alla voi olla samanaikaisesti useita erilaisia palveluita, kuten nettisivu ja sähköposti. Eri palveluilla on oma porttinsa, jonka kautta kyseisen palveluun pääsee. Esimerkiksi nettisivulle on yleensä määritelty portti 80 ja sähköpostille 25.

2.2 Älykodin palvelut

Älykotiin liittyviä palveluita voidaan toteuttaa monin tavoin. Tässä luvussa kuvataan yleisimmät tavat palveluiden toteuttamiseksi.

Pilvipalvelulla tarkoitetaan lähiverkon ulkopuolella olevaa tietoteknistä palvelua, jota käytetään yleensä internetin kautta. Pilvipalveluita voidaan toteuttaa eri tavoin. Kolme tavallisinta toteuttamistapaa ovat

- infrastruktuuri palveluna (Infrastructure as a Service, IaaS)
- ohjelmistoalustaan palveluna (Platform as a Service, PaaS) ja
- ohjelmistoon palveluna (Software as a Service, SaaS).

IaaS-mallissa saadaan pilvipalveluna virtuaaliset laitteet, joiden käyttöjärjestelmien ja tarvittavien ohjelmistojen asennuksista ja ylläpidosta huolehtii IaaS-palvelun käyttäjä. SaaS-mallissa palvelun käyttäjä käyttää pilvipalvelua ja SaaS-palvelun tuottaja huolehtii laitteistojen ja ohjelmistojen asennuksista ja ylläpidosta. (Liikenne- ja viestintävirasto Traficom, 2019)

Erilaisten älykotilaitteiden asentamisen yhteydessä liitytään usein myös johonkin pilvipalveluun. Esimerkiksi älypuhelimen asennuksessa liitytään yleensä ainakin laitteen valmistajan pilvipalveluun ja Googlen pilvipalveluihin. Älykotilaitteissa on usein mahdollisuus liittyä laitteen valmistajan, Amazonin tai Googlen pilvipalveluihin. Älykodin käyttäjille palvelut tarjoavat esimerkiksi puheentunnistusta, virtuaaliavustajaa sekä paikka- ja säätietoja.

Eri valmistajien toteuttamien kaupallisten palveluiden lisäksi on olemassa vapaasti käytettävissä olevia palveluita ja ohjelmistoja. Osan näistä voi halutessaan asentaa omille laitteilleen ja tarvittaessa tehdä paikallisen asennuksen.

2.3 Langattomia antureiden ja laitteiden tiedonsiirtotekniikoita

Koska älykodin rakentajat todennäköisesti käyttävät langattomia laitteita, on syytä käsitellä yleisimmät älykodin käyttöön soveltuvat teknologiat. Langattomien laitteiden etuna on helppo asennus, koska johtoja ei tarvitse asentaa. Lisäksi laitteet voivat toimia myös akuilla.

Langattomien antureiden ja ohjauslaitteiden tiedonsiirtoon on tarjolla paljon erilaisia teknisiä ratkaisuja ja standardeja. Osa tekniikoista on suljettuja valmistajakohtaisia, ja osa on yleisesti eri valmistajien käytettävissä. Uudet tekniikat ovat monipuolisia, ja ne voivat itsenäisesti mukautua eri tilanteisiin ja päivittää laitteet automaattisesti.

Älykodin rakentajalle on tarjolla lyhyen ja pitkän kantaman langattomia laitteita. Lyhyen kantaman laitteet toimivat kodin piirissä, ja pitkän kantaman laitteet toimivat kilometrien säteellä.

2.3.1 Lyhyen kantaman langaton tiedonsiirto

Älykodin eri toimintoihin sopivia Zigbee-laitteita on markkinoilla tuhansia, ja niitä valmistavat esimerkiksi Philips, Osram, Samsung ja Ikea. Zigbee- versioita on useita erilaisia, eivätkä vanhat Zigbee-laitteet välttämättä

ole keskenään yhteensopivia. Zigbee-laitteet muodostavat automaattisesti itsekorjautuvan MESH-verkon. (Zigbee Alliance, 2019)

Z-Wave-teknologia on suunniteltu erityisesti kiinteistöjen laitteiden ohjaukseen ja tiedonkeruuseen. Suomessa erilaisia Z-Wave-laitteita tarjoavat esimerkiksi Samsung, Nexa, Teldus ja Fibaro. Z-Wave-standardien mukaan eri valmistajien laitteet ja eri sukupolvien laitteet ovat keskenään yhteensopivia. Z-Wave laitteet muodostavat MESH-verkon. (Z-Wave Alliance, 2019)

WiFi on yleisesti käytössä kodeissa ja yrityksissä lähes kaikenlaisten laitteiden langattomaan tiedonsiirtoon. Älykodin käyttöön soveltuvia WiFi-laitteita on paljon saatavilla, ja ne voidaan helposti liittää suoraan kodin WiFi-verkkoon. Uudet WiFi-versiot tukevat myös MESH-verkkoa.

Bluetooth-laitteita on ollut markkinoilla yli kaksikymmentä vuotta, ja erilaisia Bluetooth-laitteita on paljon. Vuonna 2020 arvioidaan valmistettavan yli neljä miljardia laitetta, joissa on Bluetooth. Esimerkiksi matkapuhelimissa, kannettavissa tietokoneissa, kodin viihde-elektroniikassa ja monissa älylaitteissa käytetään Bluetooth-tekniikkaa. Bluetoothista on julkaistu useita eri versioita, ja käytössä on kaksi eri radioteknologiaa, Bluetooth Classic ja Bluetooth Low Energy (LE). Bluetooth LE tukee myös MESH-verkkoa. (Bluetooth SIG, 2020) Bluetooth sopii hyvin älykodin laitteita varten. Markkinoilla on saatavilla esimerkiksi valaisimia, kaiuttimia, mediatoistimia ja paristoilla toimivia antureita.

LPD433-laitteita (Low Power Device 433 MHz) myyvät esimerkiksi Nexxa ja Teldus. Teknologiaa on käytetty langattomissa autonavaimissa, sääasemissa ja edullisissa kauko-ohjatuissa pistorasioissa. LPD433 on vanha ja ominaisuuksilta rajoittunut teknologia. Monessa kodissa on yhä käytössä kauko-ohjattavia pistorasioita, jotka on todennäköisesti tehty LPD433-teknologialla. Valmistajat ovat kuitenkin siirtyneet käyttämään uusia tekniikoita. Vanhojen laitteiden hyödyntäminen älykodin rakentamisessa vaatisi vanhaa tekniikkaa tukevan reitittimen.

2.3.2 Pitkän kantaman langaton tiedonsiirto

IoT-tiedonkeruuta varten on kehitetty erilaisia vähävirtaisia, pitkän kantaman langattomia tiedonsiirtotekniikoita. Niitä voi hyödyntää myös älykodin rakentamisessa. Laitteet voivat toimia akulla ilman erillistä virransyöttöä jopa yli kymmenen vuotta.

LoRaWAN on vapaasti kenen tahansa käytettävissä oleva teknologia. Halutessaan älykodin rakentaja voi tehdä oman LoRaWAN-verkon tai käyttää valmiita LoRaWAN-verkkoja. (LoRa Alliance, 2019) Suomessa Digita tarjoaa yrityksille valtakunnallista LoRaWAN-verkkoa, jota käyttäen eri yritykset ovat tehneet kuluttajillekin suunnattuja palveluja.

Älykodin rakentajalle on tarjolla paljon erilaisia LoRaWAN-antureita ja -laitteita. LoRAWAN-verkossa voi tiedon perillemeno kestää pari sekuntia, joten esimerkiksi valojen ohjaukseen se ei ole välttämättä hyvä vaihtoehto.

NB-IoT ja LTE-M toimivat teleoperaattoreiden matkapuhelinverkossa. Suomessa operaattorit eivät tarjoa NB-IoT- ja LTE-M-ratkaisuja kuluttajille. Globaaleilla markkinoilla on useita IoT-tiedonsiirtoratkaisuja tarjoavia yrityksiä, joilta voi tilata Suomessakin toimivan NB-IoT- ja LTE-M-yhteyden. Esimerkiksi tanskalainen ConnectedYou yritys tarjoaa DNA:n ja Telian LTE-M-verkoissa toimivan SIM-kortin hyvin edulliseen hintaan, jopa yksin kappalein tilattuna. Tätä opinnäytetyötä tehdessä ei Suomesta ollut löydettävissä älykodin rakentajalle tarjolla olevia NB-IoT- ja LTE-M-laitteita.

Sigfox on yksi yhtenäinen globaali tiedonsiirto, jota operoi ranskalainen yritys. Suomessa Sigfox-verkon palveluita tarjoaa Connected Finland Oy, mutta palveluita tarjotaan vain yrityksille. Sigfox soveltuu hitaaseen ja muutaman kerran tunnissa tapahtuvaan tiedonkeruuseen. Tällä hetkellä Sigfox-ratkaisuja ei tarjota kuluttajille, mutta vuonna 2021 Sigfox on tuomassa markkinoille Sigfox Private Area Network -vaihtoehtoa, jossa käyttäjä saa oman reitittimen ja mahdollisuuden tallentaa dataa paikallisesti. (Sigfox, 2020)

5G-teknologialla luvataan olevan mahdollista toteuttaa paristolla toimivia tiedonkeruu- ja ohjauslaitteita, joita voi nykytekniikoihin verrattuna olla pienellä alueella todella paljon. 5G-teknologioiden yhteydessä onkin alettu puhua Internet of Everything- ja Massive IoT -ratkaisuista. Älykodin käyttöön tarkoitettuja 5G-laitteita ei ole vielä saatavilla, mutta on todennäköistä, että niitä tulee pian tarjolle.

2.4 Markkinoilla olevat älykotiratkaisut ja testiympäristön valinta

Tätä opinnäytetyötä varten selvitettiin ensin älykodin rakentajalle tarjolla olevia ratkaisuja. Selvitystyön yhteydessä kävi ilmi, että älykotimarkkinat ovat parin viime vuoden aikana monipuolistuneet varsin nopeasti. Uusia laitteita ja tekniikoita on tullut tarjolle paljon, ja ne ovat myös halventuneet merkittävästi. Helppoja, edullisia paketteja on saatavilla jopa lähimarketeista.

Valmiiden kaupallisten ratkaisujen lisäksi selvitettiin myös avoimia, erilaisten yhteisöjen tekemiä ja ylläpitämiä älykotiratkaisuja.

2.5 Kaupallisia älykodin alustoja

Monella valmistajalla on tarjolla kaupallisia älykotiratkaisuja, joita on helposti saatavilla sekä kodinkoneliikkeistä että päivittäistavarakaupoista.

Muun muassa Philips, Samsung, Google ja Ikea tarjoavat laadukkaita tuotteita ja valmiita peruspaketteja, joiden asennuksesta ja käyttöönotosta on pyritty tekemään mahdollisimman helppoa.

Tätä opinnäytetyötä varten tehdyissä testeissä kokeiltiin asentaa eri valmistajien palveluita. Testeissä todettiin, että kaupallisten sovellusten asentaminen on tehty vaivattomaksi. Esimerkiksi Ikean älykotipaketti asennetaan kännykän sovelluksella, joka opastaa visuaalisesti, mitä eri vaiheissa pitää tehdä. Perusasennuksien lisäksi helpoksi on tehty myös liittyminen esimerkiksi Googlen palveluihin, kuten puheentunnustus- ja virtuaaliassistenttipalveluihin. Vaikka suurin osa kaupallisista ratkaisuista ovat helppokäyttöisiä, ne ovat kuitenkin usein muokattavuudeltaan rajallisia. Osa eri valmistajien laitteista vaikuttaa olevan keskenään yhteensopivia, mikä on kuluttajan kannalta merkittävä asia.

Älykotiratkaisujen vaihtoehtoja selvitettiin käymällä kaupoissa sekä tutkimalla verkkokauppojen valikoimaa. Aiemmin älykotiratkaisuna myytiin lähinnä valaistusten ohjausta. Nyt kuitenkin havaittiin, että tarjolla on jo laajoja älykotiratkaisuja, joilla voi tehdä muutakin kuin ohjata valaistusta. Nykyään on mukana esimerkiksi multimedian, ilmastoinnin ja lämmityksen ohjausta. Huomattiin myös, että hintataso on parissa vuodessa laskenut merkittävästi. Esimerkiksi Ikea on tuonut markkinoille erittäin edullisia laitteita.

2.6 Avoimia älykodin alustoja

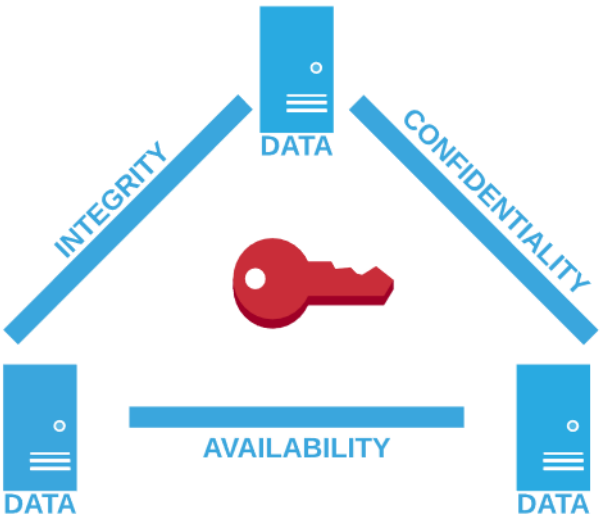
Hakemalla internetistä avoimeen lähdekoodiin perustuvia älykotialustoja voi huomata, että niitä on todella paljon. Avoimen lähdekoodin alustoja on usein ollut tekemässä suuri joukko henkilöitä ja organisaatioita. Yhteistä kaikille on luonnollisesti se, että niihin liittyy käyttäjän mahdollisuus tehdä omia muokkauksia.

Internetistä löytyy hakusanalla ”Smart Home” helposti useita kymmeniä erilaisia avoimia älykotialustoja. Eri toteutuksissa on keskitytty eri asioihin. Esimerkiksi osassa keskitytään automaatioon ja osassa käytön helppouteen. Eri älykotiratkaisuista monipuolisimmilta ja hyvin tuetuilta vaikuttivat openHAB, Home Assistant ja Mozilla WebThings. Niissä oli selkeät käyttöliittymät ja laaja tuki erilaisille laitteille. Ne voi asentaa esimerkiksi PC- ja MAC-tietokoneelle, virtuaalikoneelle tai Raspberry PI -laitteelle.

Selvitettyjen vaihtoehtojen perusteella näyttää siltä, että avoimen lähdekoodin ratkaisuilla voi toteuttaa helppokäyttöisen ja ominaisuuksiltaan monipuolisen älykodin.

2.7 Tietoturva ja kyberturvallisuus

Tietoturvalla pyritään varmistamaan tiedon luottamuksellisuus (confidentiality), eheys (integrity) ja saatavuus (availability). Englanninkielisten sanojen alkukirjaimista muodostuu lyhenne CIA. (Järvinen, 2002, s. 22) CIA-malli voidaan esittää kolmiona (Kuva 1).



Kuva 1. Tietoturvan CIA-malli (Kyamk, 2018, muokattu).

Turvallisuuskomitean sihteeristö, Huoltovarmuuskeskus ja Sanastokeskus TSK ovat yhteisprojektissaan määrittäneet eri kyberturvallisuus- ja tietoturvakäsitteille suomenkieliset termistöt, jotka on julkaistu Kyberturvallisuuden sanastona (Sanastokeskus TSK ry, 2018). Sanaston määritelmän (s. 22) mukaan kyberturvallisuus on ”tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan”. Kybertoimintaympäristön puolestaan määritellään olevan ”yhdestä tai useammasta digitaalisesta tietojärjestelmästä muodostuva toimintaympäristö” (s. 21).

Monet eri palvelut ja ohjelmistot haluavat kerätä erilaista tietoa käyttäjistä ja laitteista. Kerätyt tiedot ovat yrityksille arvokkaita, ja tiedoilla yritykset tekevät erittäin tuottoisaa liiketoimintaa. Esimerkiksi Google kerää palveluidensa käyttäjistä paljon tietoja, joiden perusteella Google kohdentaa yhteistyökumppaneidensa mainontaa (Google, 2020). Ajan mittaan tietoa yksittäisestä käyttäjästä kertyy niin paljon, että siitä muodostuu yksilön identiteetin kannalta merkittävä tietoturvariski.

Jopa suurten valmistajien tuotteiden tietoturvaa ja toimintatapoja on vaikea arvioida. Esimerkiksi Samsungin SmartThings-älykotiratkaisu onkin Samsungin omistaman tytäryhtiön tuote. Tytäryhtiö sijaitsee Kaliforniassa, jolloin tietojen käsittelyssä ja viranomaisyhteistyössä toimitaan Yhdysvaltain säännösten mukaan. (SmartThings Inc, 2020) Jos Yhdysvalloissa olevalle datalle halutaan tehdä jotain, ei suomalainen tai eurooppalainen lainsäädäntö käyttäjää suojaa. On jo uutisoitu tapauksesta, jossa Yhdysvaltain

viranomaiset ovat ostaneet kaupallisen toimijan markkinointiyhtiöiltä ostettua dataa. Hankitun datan perusteella on jäljitetty paperittomia siirtolaisia. (Nurminen, 2020).

Haavoittuvuus altistaa tietoturvan erilaisille uhkille. Älykodissa haavoittuvuuksia voi olla ohjelmistoissa, laitteissa ja toimintatavoissa. Tietoturvan saattaa vaarantaa esimerkiksi niin, että asennuksen yhteydessä jättää tarkat malli- ja ohjelmistoversiotiedot näkyville. Sellaisia haavoittuvuuksia, joihin ei ole vielä saatavilla korjausta, kutsutaan nimellä nollapäivähaavoittuvuus (Sanastokeskus TSK ry, 2018).

3 TESTIYMPÄRISTÖ

Testiympäristöä valittaessa painotettiin helppokäyttöisyyttä, monipuolisuutta ja tietoturvaa. Lisäksi testiympäristön oli oltava avointa lähdekoodia. Home Assistant vaikutti testiympäristöä varten sopivimmalta, joten asennukset päätettiin tehdä sillä.

Home Assistant on GitHub-ohjelmistokehitysalustan aktiivisimpia projekteja. GitHub-ohjelmistoalustan mukaan Home Assistantia on kehittämässä 6300 ohjelmoijaa. (GitHub Inc., 2019) Projektin tavoitteena on luoda helppokäyttöinen kotiautomaatiototeutus, joka käyttää avoimen lähdekoodin ohjelmistoa ja takaa yksityisyyden. Lisäksi sen voi halutessaan yhdistää erilaisiin pilvipalveluihin. (Home Assistant, 2020)

Home Assistant -projektissa oli vuoden 2019 loppuun mennessä tehty yli 1500 integraatiota erilaisiin laitteistoihin, ohjelmistoihin ja palveluihin. Integraatioita on tehty esimerkiksi AI-projekteihin, joiden kautta on mahdollista toteuttaa vaikkapa puheohjaus kokonaan omilla koneilla ja ilman internetyhteyttä. (Home Assistant, 2020)

Home Assistantin perustajat ovat myös perustaneet Nabu Casa -nimisen yrityksen, jonka kautta Home Assistant -käyttäjät voivat halutessaan saada helppokäyttöisen pilvipalvelun. Palvelussa käyttäjällä on täysi kontrolli omaan dataansa ja pilvipalvelun lupaus siitä, että dataa ei myydä eteenpäin. (Home Assistant, 2020)

Älykodin ohjattavaksi laitteiksi valittiin Ikean valikoimista löytyviä Trådfri-sarjan laitteita. Niitä myydään paljon, ja oletettavasti moni ottaa laitteet käyttöön ajattelematta tietoturvaa. Kuluttajat yleisesti ostavat paljon Ikean tuotteita, joten on tärkeää selvittää, millä tavalla niiden kyberturvallisuus on toteutettu. Taulukko 1 sisältää hankitut IKEA Trådfri -laitteet ja niiden ohjelmistoversiot. Taulukon tiedot on koottu Ikean tuotetiedoista ja asennusohjelman versiotiedoista.

Taulukko 1. IKEA Trådfri -laitteiden mallit ja versiot.

Laite	**Malli**	**Versio**
Lamppu 1	LED1733G7	2.0.022
Lamppu 2	LED1733G7	2.0.022
Liikkeen tunnistin	E1745	2.0.022

Kaukosäädin	E1810	2.3.014
Pistorasia	E1603	2.0.022
Reititin	E1526	1.9.27

3.1 Testiympäristön asennus

Testiympäristön asennus alkoi asentamalla Ikean laitteet niiden mukana tulleiden ohjeiden mukaisesti. Ohjeet olivat hyvät ja selkeät, ja asennus onnistui niiden avulla vaivatta. Koska opinnäytetyön tarkoituksena ei ollut tutkia erilaisia älykotitoimintoja, Ikean laitteille ei tehty perusasennuksen jälkeen muita testauksia.

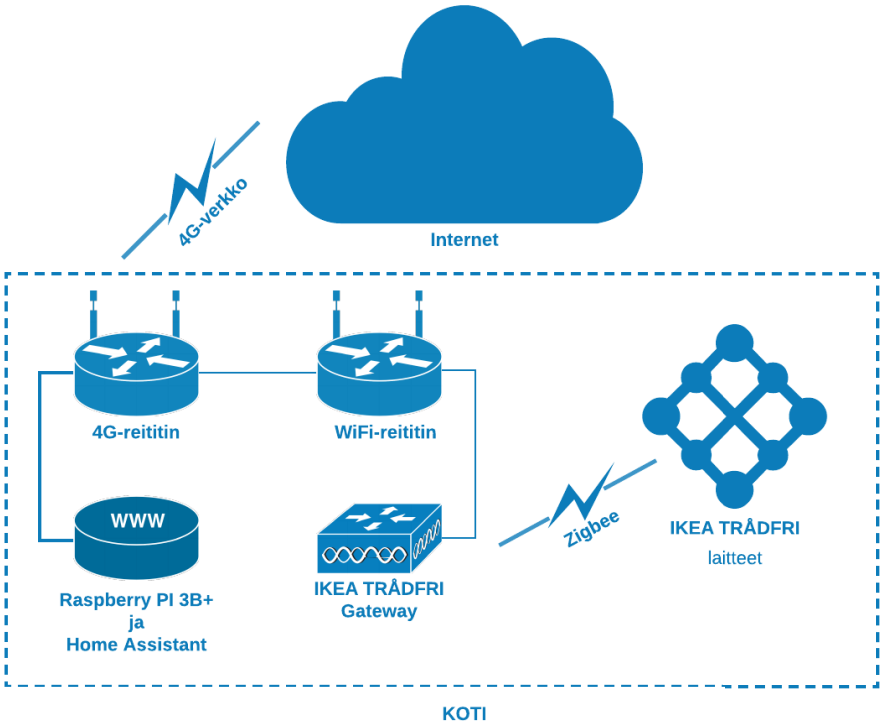
Ikean reititin kytkettiin ethernet-kaapelilla suoraan WiFi-tukiasemaan, ja ohjattavat Ikean laitteet liitettiin Zigbee-yhteydellä reitittimeen. Asennuksen yhteydessä reititin hakee itselleen DHCP:n avulla automaattisesti IP-osoitteen. Sitä ja muita reitittimen tietoliikenneasetuksia ei pääse suoraan selaimella tai sovelluksella muuttamaan. Reitittimeen ei saa yhteyttä selaimen kautta, vaan kaikki asetukset tehdään Ikea Home Smart -sovelluksella.

Ikean reitittimeen liitettävien laitteiden asennusta varten tarvitaan tabletti tai matkapuhelin, ja siihen täytyy ladata Googlen Play-kaupasta Ikea Home Smart -sovellus. Kuva 2 näkyy asennuksen yhteydessä tarvittavia turvakoodeja. Ikean reitittimen ja Ikean laitteiden välillä käytetään langatonta Zigbee-teknologiaa.

Kuva 2. IKEA Trådfri -reititin.

Älykodin keskusyksiköksi hankittiin edullinen Raspberry PI 3B+ -korttitietokone, jossa on valmiina WiFi- ja Bluetooth BLE 4.2 -ominaisuudet. Ohjelmistojen asennusta varten hankitiin riittävän iso muistikortti, jolle asennettiin valittu Home Assistant -ohjelmisto.

Internetyhteyttä varten käytettiin kodissa valmiina olevaa 4G-reititintä. Reitittimessä olevaa WiFi-tukiasemaa ei käytetty, vaan WiFi-tukiasemana oli erillinen Ubiquiti-laite. Kuva 3 on kaavio tehdystä asennuksesta.



Kuva 3. Kaavio järjestelmästä.

Älykodin ohjaukseen käytettiin kodissa valmiina olevia tietokoneita, tabletteja ja matkapuhelimia. Vertailun vuoksi älykodin ohjauksia tehtiin eri sovelluksilla ja internetselaimilla.

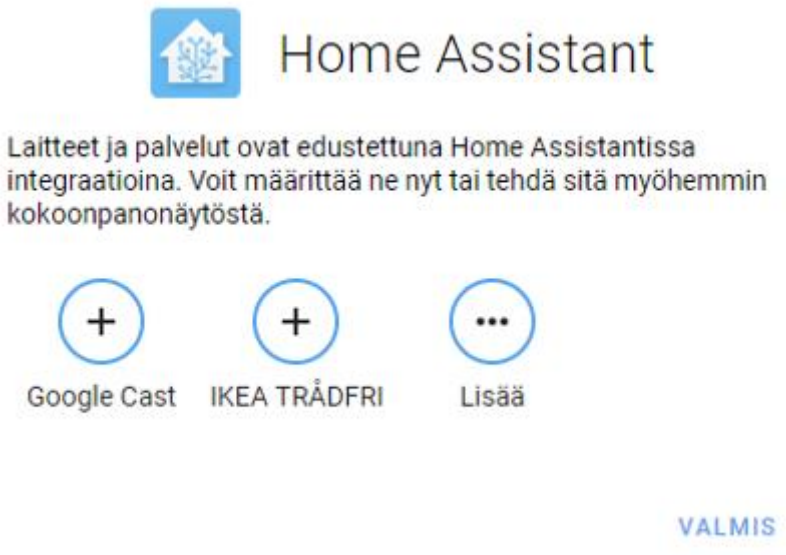
3.2 Home Assistant -ohjelmistojen asennus

Home Assistant -ohjelmiston asennuksesta on Home Assistant -sivustolla hyvät ohjeet. Ohjeiden avulla ohjelmistojen asennus on helppoa. Asennusta varten on tehty valmiit asennuspaketit, jotka sisältävät tarvittavan käyttöjärjestelmän ja asennettavat ohjelmat. Asennuspaketeista on versioita virtuaalikoneille, Intel NUC -tietokoneelle ja eri Raspberry PI -laitteille.

Valmis asennuspaketti kopioitiin muistikortille, minkä jälkeen laitettiin muistikortti Raspberry Pi 3 B+ -laitteeseen. Ensimmäisen käynnistyksen yhteydessä Home Assistant päivitti ohjelmistot ja etsi automattisesti kotiverkosta löytyvät laitteet. Tämä vaihe kesti parikymmentä minuuttia.

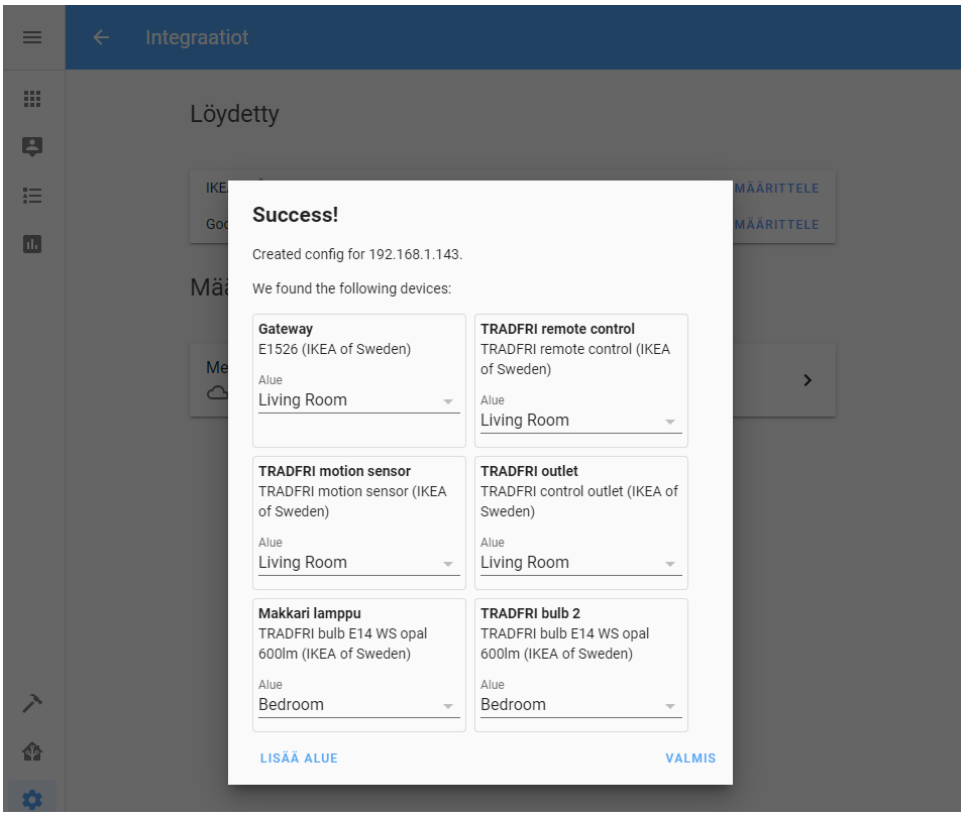
Kun Home Assistant -asennus oli valmiina, mentiin ohjeiden mukaisesti selaimella osoitteeseen http://hassio.local:8123. Osoitteesta aukeaa Home Assistant -kirjautumissivu. Kirjautumissivulla määriteltiin pääkäyttäjän käyttäjätunnus ja salasana.

Seuraavalla sivulla määriteltiin pyydetysti sijainti, korkeus merenpinnasta, käytettävä yksikköjärjestelmä sekä pituuden ja lämpötilan yksikkö. Tarkkojen sijaintitietojen perusteella voidaan esimerkiksi määritellä auringon nousu- ja laskuaikoja tai säätietoja.
Paikkatiedon määrittelyn jälkeen Home Assistant ehdotti löytämiensä laitteiden asentamista (Kuva 4). Home Assistantin annettiin tehdä asennukset automaattisesti.



Kuva 4. Laitteet ja palvelut.

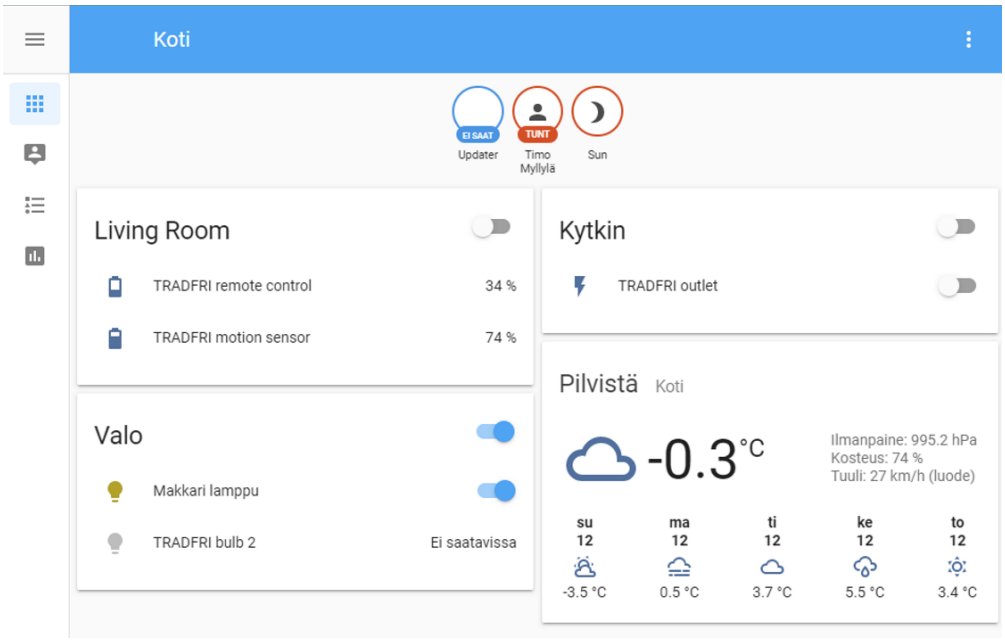
Home Assistant tunnistaa suoraan IKEA Trådfri -reitittimen ja pyytää yhteyden muodostamista varten reitittimen pohjasta löytyvän turvakoodin. Turvakoodin syöttämisen jälkeen tulee listaus reitittimeen liitetyistä laitteista. Kuva 5 näkyy, että kaikki kytketyt laitteet löytyivät.



Kuva 5. Kytketyt laitteet.

Asennusohjelma hakee paitsi laitteet, myös reitittimeen Ikea Smart Home -ohjelmalla tehdyt asetukset. Mahdollisesti myöhemmin Ikean reitittimeen liitetyt laitteen saa lisätyksi automaattisesti käynnistämällä Raspberry PI:n uudelleen. Laitteiden lisäämisen jälkeen perusasennukset ovat valmiina, ja laitteita voi ohjata kotiverkossa selaimella.

Kuva 6 on Home Assistantin aloitusnäkymä, jonka asennusohjelma teki automaattisesti. Näkymä on responsiivinen, eli se skaalautuu automaattisesti eri kokoisia näyttöjä varten. Näkymää voi myös muokata, ja siihen voi lisätä erilaisia elementtejä.



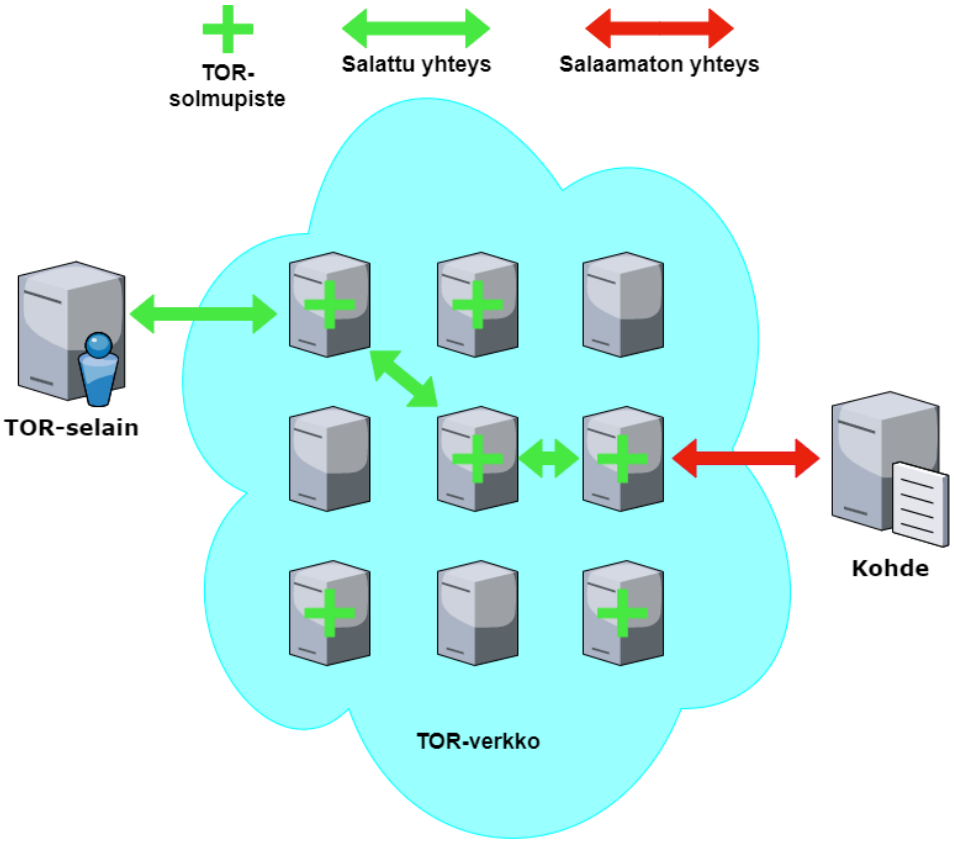
Kuva 6. Home Assistantin perusnäkymä.

3.3 Etäyhteyden asennus ja konfigurointi

Etäyhteyden tekemiseksi selvitettiin ja kokeiltiin erilaisia vaihtoehtoja, mutta monet ratkaisut eivät olleet riittävän yksinkertaisia asentaa eivätkä helposti ylläpidettävissä. Etäyhteyden muodostamiseen liittyy paljon erilaisia palveluita ja asetuksia, joilla määritetään tietoliikenteen ohjauksia ja salauksia.

Yhtenä vaihtoehtona etäyhteyden toteuttamiseksi selvitettiin mahdollisuutta tehdä Home Assistant asennuksesta vain TOR-verkossa näkyvä, normaalista internetistä piilotettu asennus. TOR-verkko on vapaaehtoisten ylläpitämä tietoliikenneverkko, jossa tieto kulkee salattuna monen pisteen kautta. TOR-verkon avulla saadaan salattua tietoliikenteen alkuperä ja käyttäjä (Electronic Frontier Finland ry, 2020). TOR-verkosta käytetään myös nimityksiä pimeä verkko ja anonyymi verkko. Englanninkielisiä nimityksiä TOR-verkolle ovat Deep Web ja Dark Web.

Tietoliikenteen suojaaminen tehdään salaamalla tietoliikenne ja reitittämällä se kolmen satunnaisen solmupisteen (Tor Noden) kautta, joista kukin näkee vain seuraavan solmupisteen. **Virhe. Viitteen lähdettä ei löytynyt.** on esitetty TOR-verkon rakenne ja tiedonkulku. Yhtä reittiä käytetään noin kymmenen minuuttia, minkä jälkeen yhteys reititetään uudelleen kolmen eri solmupisteen kautta. (The Tor Project, 2020)



Kuva 7. TOR-verkko (Electronic Frontier Finland ry, 2020, muokattu).

TOR-verkossa on erilaisia palveluita sellaisille henkilöille, jotka tarvitsevat erityistä yksityisyydensuojaa ja anonymiteettia. Tällaisia ihmisiä voivat olla esimerkiksi opposition edustajat, vähemmistöryhmiin kuuluvat henkilöt tai kansalaiset sellaisissa maissa, joissa sananvapautta on rajoitettu. (Electronic Frontier Finland ry, 2020)

TOR-verkossa on paljon erilaisia palveluita, kuten sähköposti, tiedonsiirtopalveluita, keskustelupalstoja, kirjastoja ja sanomalehtien verkkoversioita. Esimerkiksi Facebook ja BBC ovat myös TOR-verkossa. Facebook on osoitteessa (https://www.facebookcorewwwi.onion/) ja BBC osoitteessa (https://www.bbcnewsv2vjtpsuy.onion/). TOR-verkossa sijaitsevat sivut ovat hyödyllisiä esimerkiksi sellaisten maiden kansalaisille, joilta on estetty pääsy sivustolle internetin kautta.

Valitettavasti TOR-verkon yksityisyyden suojaa ja anonymiteettiä käytetään hyväksi myös rikollisessa ja muussa arveluttavassa toiminnassa. Esimerkiksi Suomessa on uutisoitu ja kirjoitettu TOR-verkossa tapahtuvasta huumekaupasta. (Poliisi, 2017)

Tässä opinnäytetyössä hyödynnettiin TOR-verkon ominaisuuksia turvallisen etäyhteyden muodostamiseksi. Erilaisia TOR-sivuston asennusoppaita on internetissä runsaasti tarjolla, ja Home Assistant -sivustolla on myös suoraan asennusoppaat TOR-yhteyksien käyttämisestä. Tarjolla on myös valmis Home Assistantia varten tehty lisäosa, jonka käyttöönotto ja hallinta vaikuttavat suoraviivaisilta.

Asennusohjeissa neuvottiin tekemään konfiguraatiotiedostoon omat asetukset, mutta asennus tehtiin konfiguraatiotiedoston oletusarvoilla. Asetuksilla on mahdollista parantaa tietoturvaa. Silloin tosin yhteydenkin muodostamista varten joutuu muuttamaan TOR-selaimen asetuksia.

Lisäosan asennuksen ja käynnistyksen jälkeen lokitiedostossa on seuraavat rivit, joissa on asennuksen yhteydessä muodostunut TOR-verkossa .onion-osoite:

[11:06:12] INFO: ----------
[11:06:12] INFO: Your Home Assistant instance is available on Tor!
[11:06:12] INFO: Address: xyz1234.onion
[11:06:12] INFO: ----------

Lokitiedostossa näkyvän .onion-osoitteen perään on lisättävä myös Home Assistant -asennuksen käyttämä portti. Oletuksena Home Assistant käyttää porttia :8123, eli asennuksen jälkeen tehty Home Assistant asennus löytyy TOR-selaimella osoitteesta xyz1234.onion:8123.

Sivustolla (https://www.torproject.org/) on TOR-selaimen lataus- ja asennusohjeet eri laitteille ja käyttöjärjestelmille. Asennuksessa käytettiin TOR-selainta Windows 10- ja Android-laitteilla. Yleensä TOR-selaimella liitytään ensin TOR-verkkoon, minkä jälkeen TOR-selainta voi käyttää kuten tavallista selainta.

3.4 Testiympäristön toiminnan arviointi

Testiympäristöstä oli eri versioita käytössä päivittäin kolmen kuukauden ajan. Sinä aikana kokeiltiin erilaisia tapoja saada etäyhteys tietoturvallisesti kodin ulkopuolella tabletilla tai matkapuhelimella.

Testauksen aikana ei havaittu luotettavuusongelmia eikä laitteisiin tullut vikoja. Etäyhteydellä käytettävyys oli huonompi kuin suoraan kotona muodostettu yhteys. Kotiverkon sisällä voi käyttää tavallista selainta tai Home Assistant -sovellusta, jotka ovat nopeampia. Toiminnot kyllä toimivat etäyhteydelläkin, mutta ruudun päivitys oli hitaampi ja toimintojen tapahtumista joutui hieman odottamaan. Eniten vei aikaa kirjautuminen. Salatun etäyhteyden muodostaminen vei aikaa keskimäärin 15 sekuntia. Käytettävyys arvioitiin kuitenkin kokonaisuudessaan riittävän hyväksi.

Myös Home Assistantin omaa matkapuhelimelle ja tabletille tarkoitettua sovellusta testattiin. Kotikäytössä sovellusta voi käyttää paikallisesti ilman kytköstä ulkopuoliseen palveluun. Sovelluksen avulla älykotia pääsee ohjaamaan nopeasti ilman erillistä kirjautumista, mikä on hyvä asia. Muutoin älykodin ominaisuudet jäävät helposti hyödyntämättä.

Oletusasetuksillakin Home Assistantin käyttöliittymä on selkeä ja helppo. Eri toiminnot on selvästi ryhmitelty, ja näkymä skaalautuu eri kokoisiin näyttöihin. Joissain kohdissa valikkojen suomen kieli on hieman kankeaa, joten kieliasua on syytä vielä kehittää.

Automaatioita tai erilaisia älykkäitä toimintoja ei testauksen aikana tehty, joten niiden toiminnasta ei saatu vielä kokemuksia. Home Assistantissa tosin on valmiit konfigurointityökalut, joilla erilaisia toimintoja voi rakentaa ilman ohjelmointia.

Testauksen aikana syntyi paljon ideoita, joita voi myöhemmin toteuttaa. Esimerkiksi matkapuhelimen avulla käyttäjän kotiintulo on helppo tunnistaa, ja eteisen valot voi ohjata tunnistuksen perusteella automaattisesti.

3.5 Testiympäristön kyberturvallisuus

Testiympäristön kyberturvallisuus on laitteiden, palveluiden ja käyttöympäristön muodostama kokonaisuus. Älykotilaitteiden käyttämät monet erilaiset tekniikat ja standardit tekevät kokonaisuuden hallinnasta vaikean. Pahimmillaan yhden vanhentuneen komponentin tai ohjelmiston käyttäminen saattaa vaarantaa koko älykotiratkaisun turvallisuuden.

Seuraavaksi käsitellään sellaisia kyberturvallisuusasioita, joita älykodin rakentaja todennäköisimmin kohtaa ja joihin hän voi myös vaikuttaa.

3.5.1 Komponenttien ja palveluiden kyberturvallisuus

Yhtenä tavoitteena oli toteuttaa helppokäyttöinen ja tietoturvallinen etäyhteys ilman kaupallisia palveluita. Tämä toteutui testatulla TOR-yhteydellä. TOR-yhteyden voisi tehdä vieläkin turvallisemmin, mutta silloin käytettävyys kärsisi, koska TOR-selaimeen pitäisi tehdä vielä käsin lisäasetuksia.

Vuosien saatossa on ollut erilaisia tietoturvavuotoja, joissa ihmisten sähköpostiosoitteita, salasanoja ja muita yksilöiviä tietoja on päätynyt massoittain vääriin käsiin. Testiympäristössä käytössä ollut sähköpostiosoite on ollut mukana myös tietoturvavuodoissa, mutta kaikissa palveluissa käytettiin erittäin vahvoja salasanoja. Salasanojen hallintaan käytettiin erillistä, siihen tarkoitukseen suunniteltua työkalua.

Vaikka sähköpostiosoite onkin vuotanut, ei asiaa nähty ongelmaksi, koska viimeinenkin tietovuodossa paljastunut salasana on vaihdettu. Lisäksi Home Assistant tukee monivaiheista tunnistautumista.

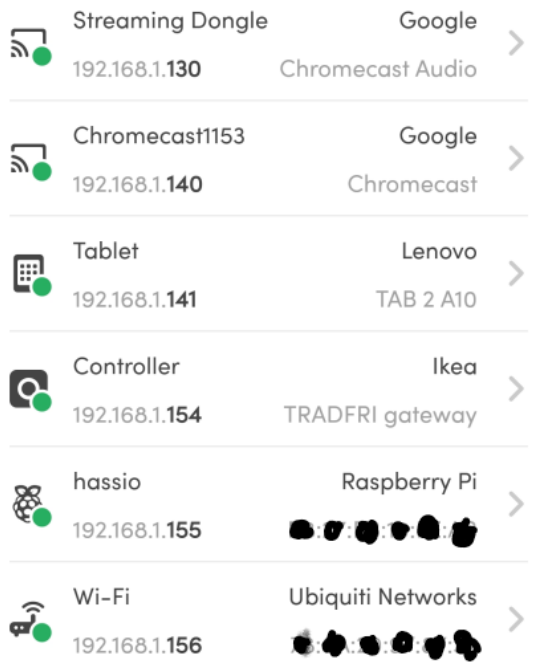
Ikean reitittimen ja Home Assistantin välinen tiedonsiirto toimii paikallisesti ja ilman internetyhteyttä. Myös se lisää tietoturvallisuutta, koska tiedon ei tarvitse välittyä kodin ulkopuolelle. Ikean reititin voisi toimia myös ilman internetyhteyttä, mutta sille jätettiin mahdollisuus tehdä automaattisia päivityksiä internetin kautta.

Yleensä kaupallisten älykotiratkaisujen ongelmana on pilvipalvelu, jossa käyttäjällä ei ole vapaata pääsyä omiin datoihinsa eikä mahdollisuutta kontrolloida datan käsittelyä tai yksityisyyteen liittyviä asioita. Esimerkiksi Googleen tai muualle lähetettyyn dataan ei pääse kunnolla käsiksi, eikä käyttäjä siten voi halutessaan analysoida omaa dataansa tai hyödyntää sitä omissa sovelluksissaan.

3.5.2 Verkon tutkiminen

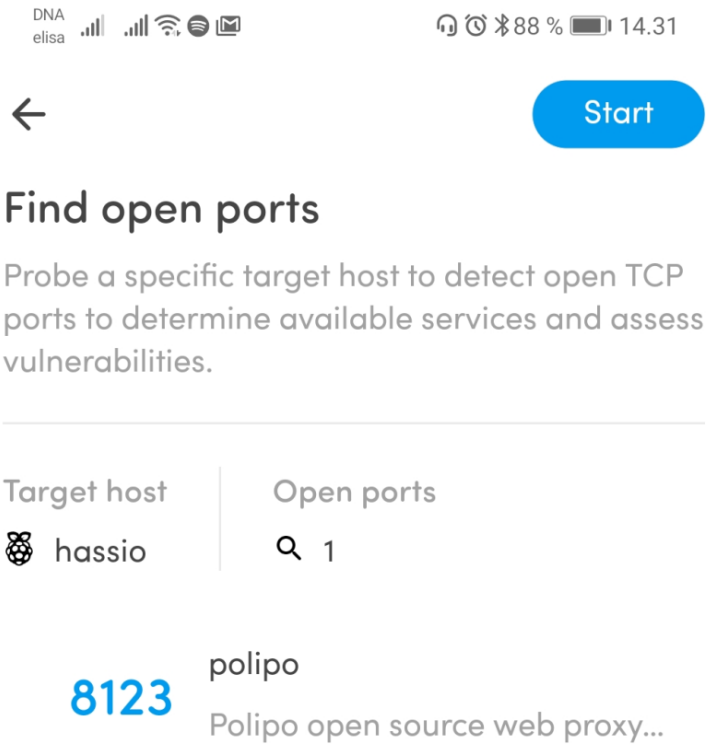
Verkon tutkimista varten on paljon erilaisia ohjelmistoja ja työkaluja. Esimerkiksi matkapuhelimeen asennettava Fing - Network Tools -sovellus (https://www.fing.com/products) on helppokäyttöinen työkalu kodin verkkoon kytkettyjen laitteiden etsimiseen ja tutkimiseen.

Fing-sovellusta testattiin tätä opinnäytetyötä varten. Kodin verkosta löytyi esimerkiksi Kuva 8 listattuja laitteita. Laitteiden tarkempia tietoja voidaan tarvita esimerkiksi silloin, kun manuaalisesti lisätään laitteita älykodin osaksi. Aika ajoin on hyvä tarkistaa kodin verkko ja tutkia, onko verkkoon liittynyt tuntemattomia laitteita.



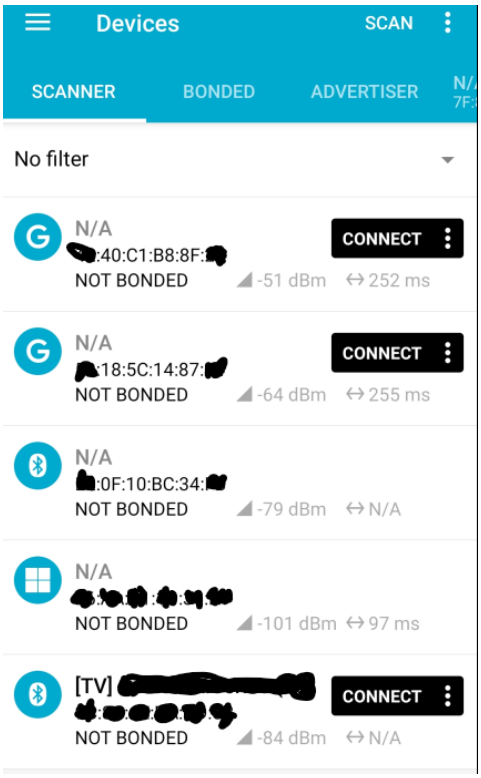
Kuva 8. Verkon laiteita.

Fing-sovelluksella tutkittiin myös eri laitteiden asetuksia. Home Assistant -asennuksesta löydettiin vain yksi avoin portti (Kuva 9). Avoimena olevan 8123-portin on tarkoitus olla avoimena, mutta muita portteja ei tarvitse olla nyt tehdyssä asennuksessa avoimena. Home Assistant käyttää normaalista poikkeavaa ja turvallista tapaa liikennöidä. Sen vuoksi internetselaimeen syötettävän osoitteen perään pitää kirjoittaa kaksoispiste ja numerosarja 8123 (esimerkiksi http://hassio.local:8123 tai xyz1234.onion:8123).



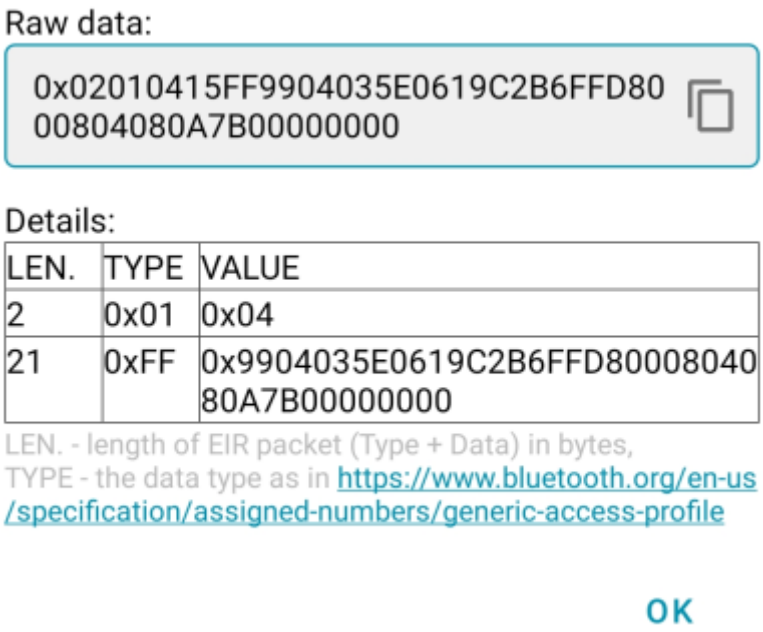
Kuva 9. Home Assistantin avoimet portit.

Koska Raspberry PI 3B+ -laitteessa on myös Bluetooth-tuki, halutiin selvittää myös sitä, millä tavoin Bluetooth-laitteiden kytkeminen testiympäristöön vaikuttaa kyberturvallisuuteen. Tätä opinnäytetyötä varten ei asennettu Bluetooth-laitteita, mutta tulevaa asennusta varten selvitettiin asennettavien Bluetooth-laitteiden MAC-osoitteita. Bluetooth-laitteiden MAC-osoitteet saatiin selville nRF Connect for Mobile -sovelluksella. Sovellus löysi odotettua enemmän laitteita. Kuva 10 on listattu osa sovelluksen löytämistä laitteista.



Kuva 10. Bluetooth-laitteita.

Listalta löytyy haluttu laite ja sen MAC-osoite, mutta listalla on myös lähiseudulla olevia vieraita laitteita. Sovelluksella on helppo selvittää myös tarkempia ominaisuuksia ja tietoliikennettä. Esimerkiksi lämpötilaa mittaavan Bluetooth-anturin mittaustiedot (Kuva 11) ovat suoraan kenen tahansa luettavissa. Se on hyvä esimerkki siitä, että erilaisten laitteiden tietoturvan taso vaihtelee suuresti. Laitteita hankkiessa on hyvä tietää laitteen tietoturvan taso, jotta voi päättää, onko laite sopiva tarkoitettuun käyttöön.



Kuva 11. Bluetooth-paketin sisältö.

Myös muiden verkkojen tutkimiseen on helposti saatavilla erilaisia ohjelmia ja laitteita. Esimerkiksi Zigbee-verkon tutkimiseen tarvitaan vain Rasberry PI, noin kolmekymmentä euroa maksava USB-laite ja internetistä ladattava ohjelma.

Helppo ja tehokas tapa lisätä tietoturvaa on olla kytkemättä älykotia internetiin, mutta silloin menetetään myös paljon hyödyllisiä ominaisuuksia. Kotiautomaation käytettävyyttä ja hyödyllisyyttä lisää mahdollisuus ottaa yhteys kotiautomaatiojärjestelmään kodin ulkopuolelta. Eri laitevalmistajat tarjoavat laitteilleen yleensä mahdollisimman helppoja tapoja ohjata laitteitaan ja liittää ne esimerkiksi osaksi Googlen palveluita.

4 SUOSITUKSIA ÄLYKODIN SUUNNITTELIJALLE JA RAKENTAJALLE

Tämän opinnäytetyön pohjalta nousi esille erilaisia älykodin suunnitteluun, tekemiseen ja käyttöympäristöön liittyviä tekijöitä, joilla voi vaikuttaa älykodin kyberturvallisuuteen. Seuraavaksi esitellään erilaisia hyödyllisiä palveluita, sovelluksia ja suosituksia älykodin toteuttamiseksi.

Monivaiheisella todentamisella tarkoitetaan käyttäjän tunnistamista vähintään kahdella eri tavalla (Sanastokeskus TSK ry, 2018). Järjestelmä voi vaatia esimerkiksi kirjautumisen ensin salasanalla ja sitten lisäksi matkapuhelimen sovelluksen avulla. Monivaiheisen todentamisen englanninkielisiä nimityksiä ovat esimerkiksi Factor Authentication, MFA ja Multi-Step Verification (Sanastokeskus TSK ry, 2018). Monivaiheista tunnistusta kannattaa käyttää aina, kun se on mahdollista.

Kotiautomaation eri laitteiden ja ohjelmistojen päivittäminen on tärkeää, koska muutoin laitteistoista ja ohjelmistoista tulee ajan myötä turvattomia. Osa laitteista päivittyy automaattisesti, mutta osaan päivitykset pitää tehdä itse. Yleensä laitetta ohjaavassa sovelluksessa on päivitystoiminto, josta käyttäjä saa tiedon saatavilla olevista päivityksistä ja jolla päivitykset voikäsin tehdä.

Ennen kuin muokkaa älykodin asetuksia tai tekee uusia asennuksia kannattaa tehdä varmuuskopio, johon voi mahdollisten ongelmien jälkeen palata. Esimerkiksi Home Assistantissa on valmiit toiminnot asetuksien varmuuskopiointiin.

Suomessa Kyberturvallisuuskeskus julkaisee tietoa ja ohjeita kyberturvallisuudesta. Ennen laitteen hankintaa ja käyttöönottoa onkin hyvä selvittää, onko laitteessa tietoturvaan liittyviä ongelmia ja onko mahdollisiin ongelmiin jo saatavilla korjaukset. Kannattaa selvittää myös, päivittääkö valmistaja laitteitaan aktiivisesti. Pienet valmistajat saattavat valmistaa erän tuotteita mutta eivät koskaan päivitä laitteita, ja seuraava erä on taas erilainen versio.

TOR-selaimella voi selailla internetiä ilman seurantaa. Erilaiset palvelut ja internetsivut keräävät usein monenlaista tietoa käyttäjistään ja sitten profiloivat käyttäjiä esimerkiksi mainontaa varten. Ylen toimittaja selvitti artikkelissaan, mihin välitetään ja kerätään tietoja käyttäjästä. Esimerkiksi Tori.fi-sivustolta lähti käyttäjätietoja 32 eri palveluun ja Twitter-palvelusta lähti käyttäjätietoja 56 eri yritykselle tai palvelulle. Artikkelissa kerrotaan myös, millaisia asioita kerätyistä tiedoista voi päätellä ja miten niitä hyödynnetään. Esimerkiksi tiedoista muodostetaan profiili, joka sisältää henkilön ominaisuuksia ja kiinnostuksen aiheita. Tämä profiili huutokaupataan mainostajille. (Hukkanen, Tuominen & Kanerva, 2019)

Suuri osa kyberturvallisuuteen liittyvistä ongelmista johtuu yhteyksistä internetiin, joten käyttäjän on pohdittava ja kontrolloitava, mitkä laitteet saavat olla yhteydessä internetiin ja millä tavoin. Reitittimen turvaominaisuuksia kannattaa hyödyntää. Älykotia varten on usein tarpeen tehdä oma

verkko, joka on erillään kodin muusta verkosta. Erillisessä verkossa olevan älykodin tietoturva-asetuksia voi kontrolloida helpommin kuin kokonaisen kotiverkon asetuksia, ja tarvittaessa voi estää kaiken muun kuin etäyhteyttä varten tarvittavan liikenteen.

Jos tiedot ovat vain yhdessä paikassa, ei ole mitään tehtävissä, jos tiedot menetetään tai niihin ei pääse käsiksi. Myös pilvipalveluissa oleville tiedoille voi tapahtua jotain. Käyttäjä voi poistaa ne vahingossa tai jokin haittaohjelma voi estää tietoihin pääsyn. Yleisenä suosituksena voidaan sanoa, että tietojen pitää olla tallennettuna ainakin kahdessa paikassa.

Markkinoille on tullut erilaisia älykodin suojaamisen tarkoitettuja tietoturvareitittimiä. Niitä valmistavat esimerkiksi F-Secure, BitDefender ja Norton. Valmistajat tarjoavat reitittimen ja kuukusimaksullisen tietoturvapalvelun. Laitteilla on helppo lisätä älykodin kyberturvallisuutta, joten niitä voi suositella peruskäyttäjälle. Tietoturvareitittimen ja ensimmäisen vuoden tietoturvapalveluin hinta on noin kaksisataa euroa (F-Secure, 2020).

Jos mahdollista, kannattaa kryptata kaikki massamuisti laitteista, jotka ovat kytkettynä internetiin. Jos kotiverkkoon tunkeudutaan, on kryptattuun massamuistiin huomattavasti vaikeampaa käsiksi kuin salaamattomaan. Monet tietokoneiden käyttöjärjestelmät sisältävät mahdollisuuden kryptata massamuisteja.

Osa kaupallisista älykotiratkaisuista ei ole yhteensopivia muiden valmistajien tuotteiden kanssa. Yhteensopimattomien tuotteiden takia voi joutua tilanteeseen, jossa on pakko käyttää yhden valmistajan laitteita ja palveluita. Kaikki eri valmistajien Z-Wave-laitteet ovat keskenään yhteensopivia (Z-Wave Alliance, 2019). Samoin eri valmistajien uusien Zigbee-laitteiden on Zigbee 3.0 -standardin mukaan oltava keskenään yhteensopivia (Zigbee Alliance, 2019). Markkinoilla on myös älykodin reitittimiä, jotka tukevat eri langattomia tiedonsiirtotekniikoita ja standardeja. Eri standardien sivuilla on myös listoja standardin mukaisista ja testatuista laitteista.

Teknologioita vertaillessa saa erilaisia vastauksia sen mukaan, mistä asiaa selvittää. Eri toimijat ja organisaatiot painottavat eri asioita ja haluavat esittää oman ratkaisun mahdollisimman edullisella tavalla. Esimerkiksi langattomista tiedonsiirtotekniikoista lähes joka valmistaja on tehnyt vertailutaulukon, jossa oma teknologia on muita parempi. Käyttäjä joutuu tekemään eri teknologioiden vertailuja itse ja päättämään siitä, mikä on hänen käyttöönsä oikea teknologia.

4.1 Palveluita ja sovelluksia älykodin rakentajalle

Tavallisesti sähköpostiviestit välitetään salaamattomina, ja ne ovat matkan varrella luettavissa. Salattua ja tietoturvallista sähköpostia varten on olemassa maksuttomia palveluita, esimerkiksi https://protonmail.com/, https://mailfence.com/ ja https://www.tutanota.com/.

Omaan kotiverkkoon kytketyt laitteet ja niiden tietoliikenneominaisuudet voi selvittää erilaisilla verkon skannausohjelmilla. Oma verkko kannattaa

aika ajoin tutkia esimerkiksi luvussa 8.2 mainitulla Fing-ohjelmalla. Näin voi varmistaa, että ulkopuolisia laitteita ei ole kytkeytynyt verkkoon. Samalla ohjelmalla voi tarkistaa myös, onko verkossa oleville tietokoneille esimerkiksi ilmestynyt lisää portteja.

Käyttäjän on myös harkittava, mihin palveluihin kirjautuu ja mitä palveluita käyttää. On myös arvioitava, miten hyvin palvelut takaavat yksityisyyden ja tietoturvan. Monista kaupallisista palveluista löytyy myös yksityisyyden takaavia vaihtoehtoja. Esimerkiksi Googlen hakukoneen sijasta voi käyttää DuckDuckGo-hakukonetta (https://duckduckgo.com/), joka ei kerää tietoa käyttäjistään. WhatsApp-viestintäsovelluksen vaihtoehdoksi käy esimerkiksi Signal-sovellus (https://www.signal.org/), joka on avointa lähdekoodia ja takaa yksityisyyden.

Koska salasanojen tietovuotoja on tapahtunut, on syytä tarkistaa, onko oma sähköpostiosoite ollut mukana tapahtuneissa tietovuodoissa. Sen voi tehdä esimerkiksi palveluissa https://monitor.firefox.com/ ja https://haveibeenpwned.com/. Samoilla sivustoilla on lista jo tapahtuneista tietovuodoista, ja sivustoilta voi tilata automaattisesti ilmoituksia uusista tietovuodoista.

Hyvät salasanat ja mahdollisuuksien mukaan kaksinkertaisen kirjautumisen käyttäminen ovat tärkeitä. Salasanojen pitää olla riittävän monimutkaisia ja yksilöllisiä, eikä samaa salasanaa pidä käyttää useassa eri paikassa. Salasanojen hallintaan on tarjolla hyviä työkaluja, joiden avulla on mahdollista hallita suurtakin joukkoa erilaisia salasanoja. Salasanojen hallintatyökaluista tutustuttiin LastPass-palveluun (https://www.lastpass.com/) ja Bitwarden-palveluun (https://bitwarden.com/). Hallintatyökaluun perustetaan tili, johon voi tallentaa käyttämänsä salasanat. Näin kaikki käyttäjän salasanat voivat olla yhden eli hallintatyökaluun kirjauduttaessa käytettävän salasanan takana. Hallintatyökalulla voi halutessaan automaattisesti kirjautua internetsivustoille ja -palveluihin.

Tämän opinnäytetyön aikana testattiin ja käytetiin LastPass-palvelua, jonka havaittiin olevan luotettava ja helppokäyttöinen. Bitwardenia ei tätä opinnäytetyötä tehdessä kokeiltu. Linux Format -lehden artikkelissa ”Set up secure password manager” käsitellään Bitwardenia ja sen käyttöönottoa. Artikkelissa kerrotaan myös, miten Bitwardenista voi tehdä oman paikallisen asennuksen. (Peers, 2020)

4.2 Älykodin rakentajan tarkistuslista

Älykodin rakentajalle on eri tahoilla tietoturvallisuuteen liittyviä ohjeita ja vinkkejä. Esimerkiksi Online Trust Alliance (OTA) on julkaisut sivustollaan älykodin tarkistuslistan. Tähän lukuun on koottu tämän opinnäytetyön tutkimusten perusteella ydinasioita, jotka ainakin on syytä tehdä ja varmistaa älykotia rakentaessa.

1. Huolehdi laitteiden ja ohjelmistojen päivityksistä.
2. Käytä kunnollisia ja yksilöllisiä salasanoja.
3. Käytä monivaiheista tunnistusta.

4. Kun otat laitteen tai palvelun käyttöön, tarkista asetukset, vaihda salasanat ja poista ylimääräiset käyttäjät.
5. Tarkista kaikkien laitteiden ja palveluiden tiedonkeruun ja jakamisen asetukset.
6. Käytä yksityisyyden ja tietoturvan takaavia palveluita.

Listassa mainittujen asioiden noudattaminen mahdollisuuksien mukaan luo hyvän alustan kyberturvalliselle kodille. Lista on luonteeltaan lyhyt muistutus tärkeistä asioista, joten siihen ei ole avattu asioiden taustoja. Niistä on kerrottu tämän opinnäytetyön aiemmissa luvuissa.

5 KEHITYSMAHDOLLISUUKSIA

Älykotien tekniikoissa, tuotteissa ja standardeissa tapahtuu nopeassa tahdissa kehitystä. Tässä luvussa esitellään muutamia mahdollisuuksia ja näkymiä, joilla voi olla merkitystä älykodin toimintaympäristölle.

Jos kodissa on jatkuvasti käynnissä oleva tietokone, sitä voi hyödyntää älykodin keskusyksikkönä. Tässä opinnäytetyössä käytetyn Home Assistant -sovelluksen voi asentaa myös tietokoneelle tai virtuaalikoneelle. Esimeriksi tietokoneelle asennettu Home Assistant, Ikean Trådfri-reititin ja Ikean Trådfri-laitteet ovat edullinen ja ominaisuuksiltaan monipuolinen kokonaisuus.

Älykodin puheenohjauksen toteuttamiseen on helppokäyttöisiä kaupallisia palveluita. On olemassa myös avoimia ja vapaasti käytettävissä olevia palveluita, joilla voi toteuttaa esimerkiksi puheentunnistus-, kuvantunnistamis-, virtuaaliassistentti- ja tekoälyratkaisuja. Niillä voi toteuttaa jopa täysin paikallisia, pelkästään kotiverkossa toimivia ratkaisuja. Esimerkiksi Stanford Universityn virtuaaliassistentti Almon https://almond.stanford.edu/ ja avoin Mycroft AI https://mycroft.ai/ ovat vapaasti käytettävissä olevia ratkaisuja.

LoRaWAN on teknisesti monipuolinen teknologia, jolla on alettu Suomessa nopeaan tahtiin toteuttaa monia isoja projekteja. Esimerkiksi Digita on uutisoinut useista vesihuollon etäluentaprojekteista (Digita Oy, 2020). LoRaWAN on hyvä vaihtoehto myös älykodin rakentajalle. LoRAWAN-laitteita on saatavilla runsaasti, ja niiden hinnat ovat nykyään edullisia. Yksi vaihtoehto LoRaWAN-laitteiden yhteyksille on The Things Network, joka on globaali avoin LoRaWAN verkko. Tähän verkkoon voi liittyä alle sadan euron reitittimellä ilman kuukausi- tai liikennöintimaksuja. (The Things Industries, 2020)

Internetissä on hakukoneita, joilla voi hakea internetiin kytkettyjä laitteita. Yksi tunnetuimmista on https://www.shodan.io/, jolla voi helposti tehdä erilaisia sanahakuja. Shodanin hakutulokset kertovat esimerkiksi IP-osoitteen, fyysisen sijainnin, haavoittuvuudet sekä sen, millaisia yhteyksiä laitteeseen voi tehdä. Erilaisia hakuja tekemällä voi Shodanin avulla tutkia omia internetiin kytkettyjä laitteita ja järjestelmiä. Shodan-hakukoneella löytää helposti esimerkiksi kiinteistöhallinnan laitteistoja, jotka eivät ole suojattuja ja joiden ohjelmistot ovat päivittämättä. Hakutuloksista voi suoraan päätellä, millaisen palvelunestohyökkäyksen kiinteistöön voisi tehdä. Kiinteistön pystyy kuitenkin helposti suojaamaan esimerkiksi tanskalaisen Secomea-nimisen yrityksen SiteManager-laitteella, joka on helppokäyttöinen ja tietoturvaltaan korkeatasoinen. Valitettavasti ratkaisu on tarkoitettu vain yrityskäyttöön eikä sitä ole tarjolla yksityishenkilöille. Secomean tietoturvatuotteesta on olemassa myös tietokoneelle asennettava versio, joka on ladattavissa valmistajan sivuilta. Versioita voi käyttää maksutta kahdella laitteella, mutta asennusta varten vaaditaan yksi kiinteä, julkinen IP-osoite.

Älykotiin liittyviä tekniikoita ja standardeja on paljon erilaisia. Tämä vaikeuttaa asennusta, hankintaa ja palveluiden kehittämistä. Eri valmistajat ja organisaatiot pyrkivät kehittämään laitteita ja standardeja yhteensopivuudeltaan ja tietoturvaltaan paremmiksi. Esimerkiksi Amazon, Apple, Google, ja Zigbee Alliance ovat perustaneet Project Connected Home over IP -nimisen työryhmän (https://www.connectedhomeip.com/), jonka tavoitteena on luoda uusi lisenssimaksuton standardi älykotilaitteiden IP-liikennöintiä varten. Projektin tavoitteena on luoda yhteensopiva ja tietoturvallinen tietoliikenne älykotilaitteiden, mobiililaitteiden ja pilvipalvelujen välille. (*Project Connected Home over IP*, 2020)

6 YHTEENVETO

Tämän opinnäytetyön tarkoituksena oli löytää ratkaisut kyberturvallisen ja käytettävyydeltään hyvän älykodin toteuttamiseksi. Suunnitteluvaiheessa oli yhtenä ajatuksena tutkia erilaisia langattomia tiedonsiirtotekniikoita ja niiden kyberturvallisuutta. Jo tausta-aineiston keräysvaiheessa täytyi todeta, että tutkimusaluetta on pakko rajata materiaalin laajuuden takia. Opinnäytetyössä keskityttiin kyberturvallisen etäyhteyden toteuttamiseen.

Taustaksi selvitettiin älykotiin liittyviä teknologioita ja saatavilla olevia ratkaisuja. Myös älykodin käyttöön soveltuvat langattomat tiedonsiirtoteknologiat kartoitettiin ja niiden soveltuvuus arvioitiin.

Testiympäristöksi asennettiin Home Assistant -älykotialusta ja laitteiksi IKEA Trådfri -sarjan tuotteita. Eniten testausta ja erilaisia asennustapoja vaati etäyhteysratkaisu. Lopulta onnistuttiin löytämään ratkaisu, joka täytti hyvin asetetut tavoitteet. Etäyhteyden luominen TOR-verkon kautta oli maksutonta, riittävän helppoa, tietoturvallista ja yksityisyyden takaavaa. Sitä voi suositella muidenkin käyttöön. Yllättävää oli se, että TOR-etäyhteyttä varten oli Home Assistantiin tehty helppokäyttöinen valmis lisäosa. Sen avulla TOR-yhteyden pystyy luomaan muutaman ohjelman asennuksella ja valmiita asetuksia käyttäen.

Opinnäytetyössä asennettiin ja testattiin erilaisia kaupallisia sovelluksia. Niiden asennuksen yhteydessä antaa helposti luvan monenlaisen käyttäjätiedon keräämiseen, eikä käyttäjä välttämättä huomaa tiedonkeruun laajuutta. Lisäksi herää kysymys siitä, kuinka moni todellisuudessa lukee eri sovellusten käyttöehdot ja tietoturvakäytännöt. Kaupalliset ratkaisut eivät yleensä erityisesti ohjaa käyttäjää miettimään tietoturva-asioita.

Testatessa vahvistui käsitys siitä, että osa langattomista laitteista on tietoturvaltaan heikkoja. Testauksissa onnistuttiin helposti keräämään langattoman anturin tietoja pelkällä kännykkäsovelluksella. Kuluttaja ei välttämättä tiedosta, että anturin mittaustiedot ovat käytännössä julkista tietoa ja kenen tahansa sellaisen henkilön luettavissa, joka on anturin kantaman piirissä.

Kokonaisuutena syntyi hyvä käsitys älykodin tekniikoista, laitteista ja mahdollisuuksista. Lopputuloksena onnistuttiin toteuttamaan käytettävyydeltään hyvä ja kyberturvallinen älykoti, johon voi muodostaa etäyhteyden. Älykodin rakentajaa varten koottiin neuvoja ja ohjeita. Lisäksi tehtiin tiivis tarkistuslista asioista, jotka jokaisen älykodin rakentajan on syytä ottaa huomioon.

Langattomille laitteille ja antureille on eri tekniikoissa määritelty tapoja laitteiden automaattiseen päivittämiseen. Yleensä päivitykset tapahtuvat automaattisesti ilman käyttäjän toimia. Olisi mielenkiintoista tutkia, miten käyttäjä voi päivityksiä kontrolloida ja millaisia tietoturvaongelmia päivityksiin liittyy. Tarkemmin voisi myös tutkia kokonaisuutena langatonta tiedonsiirtoa ja sen kybertuvallisuutta.

LÄHTEET

Åkerblom, B. (2017). *Älykkyyttä arkeen–jokapaikan tietotekniikka tulevaisuuden asuinympäristössä*. Aalto-yliopisto, arkkitehtuurin laitos.

Bluetooth SIG. (2020). *Bluetooth Technology Website*. https://www.bluetooth.com/

Digita Oy. (2020). *Ajankohtaista*. https://www.digita.fi/ajankohtaista/

Dufva, M. (2020). *Sitran selvityksia 162 tammikuu 2020*.

Electronic Frontier Finland ry. (2020). *Mikä Tor on?* http://tor.effi.org/

F-Secure. (2020). *F-Secure SENSE — Suojattu reititin ja sovellus*. https://www.f-secure.com/fi/home/products/sense

GitHub Inc. (2019). *The State of the Octoverse celebrates a year of building across teams, time zones, and millions of merged pull requests.* https://octoverse.github.com/

Google. (2020). *Tietosuojakäytäntö – Tietosuoja ja käyttöehdot*. https://policies.google.com/privacy?hl=fi

Home Assistant. (2020). *Home Assistant*. https://www.home-assistant.io/

Järvinen, P. (2002). *Tietoturva & Yksityisyys*.

Kyamk. (2018). *What is Cybersecurity*.

Liikenne- ja viestintävirasto Traficom. (2019). *Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri)*.

Liikenne- ja viestintävirasto Traficom. (2020). *tietoturvamerkki.fi*. https://tietoturvamerkki.fi/

LoRa Alliance. (2019). *LoRa Alliance home page*. https://lora-alliance.org/

Nurminen, J. (2020). *Lehti: Trumpin hallinto jahtaa paperittomia siirtolaisia ostamalla kännyköiden paikannustietoja | Yle Uutiset | yle.fi*. YLE Uutiset. https://yle.fi/uutiset/3-11199784

Poliisi. (2017). *Kaupungin varjoja - Kauppa ei aina kannata*. https://www.poliisi.fi/blogi/prime101_fi.aspx/1/1/kauppa_ei_aina_kannata_58603

Project Connected Home over IP. (2020). https://www.connectedhomeip.com/

Sanastokeskus TSK ry. (2018). *Kyberturvallisuuden sanasto*. https://turvallisuuskomitea.fi/kyberturvallisuuden-sanasto/

Sanastokeskus TSK ry. (2020). *Tietotekniikan termitalkoot*. http://www.tsk.fi/tsk/termitalkoot/fi/haku-266.html?page=index

Sigfox. (2020). *Sigfox Private Area Network Sigfox*. https://www.sigfox.com/en/private-area-network

SmartThings Inc. (2020). *SmartThings. Add a little smartness to your things.* https://www.smartthings.com/about

Talouselämä. (2019). *Älykodista paljastui turva-aukko, joka avasi hakkereille pääsyn asuntoon*. https://www.talouselama.fi/uutiset/alykodista-paljastui-turva-aukko-joka-avasi-hakkereille-paasyn-asuntoon-laitetta-myyty-20000-kotitalouteen/e3a2add7-e4d7-46f1-83f9-521c16984647

The Things Industries. (2020). *Community - The Things Network*. https://www.thethingsnetwork.org/community

The Tor Project, I. (2020). *Tor Project: Overview*. https://2019.www.torproject.org/about/overview.html.en

tivi. (2020). *Hakkeri murtautui älykodin järjestelmiin*. https://www.tivi.fi/uutiset/hakkeri-murtautui-alykodin-jarjestelmiin-tiiraili-vauvaa-ja-solvasi-vanhempia/31ce3463-0777-3e42-a67e-75c8e9887179

Virpi Hukkanen, Stina tuominen, Joel Kanerva. (2019). Toimittaja testasi: Kännykkäni laverteli minusta melkein kaiken datakauppiaille kahdessa viikossa – Koetin jäljittää, mitä tiedoilleni tapahtui. *YLE uutiset*.

Z-Wave Alliance. (2019). *Z-Wave Alliance home page*. http://www.z-wavealliance.org
Zigbee Alliance. (2019). *Home - Zigbee Alliance*. https://zigbeealliance.org/