Kodin älylukkojen tietoturvariskit

Turun yliopisto
Tietotekniikan laitos
LuK-tutkielma
Tietojenkäsittelytiede
Helmikuu 2024
Melina Väkiparta

TURUN YLIOPISTO
Tietotekniikan laitos

Melina Väkiparta: Kodin älylukkojen tietoturvariskit

LuK-tutkielma, 24 s.
Tietojenkäsittelytiede
Helmikuu 2024

Tutkielman aiheena on älylukkojen tietoturva ja niiden merkitys kodin turvallisuusratkaisuina. Tutkielmassa tarkastellaan Yale ja iLOQ -älylukkoja sekä niiden turvatoimintoja, vertaillen näiden valmistajien tarjoamia ratkaisuja. Tutkielman tarkoituksena on analysoida älylukkojen tietoturvaa OSI-mallin kerrosten näkökulmasta ja ehdottaa suojauskeinoja niiden parantamiseksi. Keskeisiä tutkimustuloksia ovat älylukkojen tietoturvariskit eri tietoturvakategorioissa sekä käytännön suojauskeinot niiden vähentämiseksi. Tulosten perusteella tehtyjen päätelmien mukaan älylukkojen käyttöön liittyy monenlaisia fyysisiä ja tietoturvariskejä, jotka vaativat huomiota kaikilla tietoturvan tasoilla. Toimenpidesuositukset sisältävät muun muassa säännöllisten laiteohjelmiston päivitysten ylläpidon, vahvan salasanan käytön kodin internet-yhteydelle ja kaksivaiheisen tunnistautumisen käytön älylukkoihin liittyvissä mobiilisovelluksissa. Lisäksi valmistajien ja palveluntarjoajien rooli turvallisten tuotteiden ja palveluiden tarjoamisessa on keskeinen. Tietoturvan näkökulmasta on kuitenkin tärkeää kiinnittää huomiota eri turvallisuusriskeihin ja soveltaa käytännön suojauskeinoja niiden vähentämiseksi tai estämiseksi. Valmistajien ja palveluntarjoajien rooli turvallisten tuotteiden ja palveluiden tarjoamisessa on keskeinen, ja käyttäjien on tärkeää olla tietoisia älylukkojen tietoturvaominaisuuksista tehdessään päätöksiä tuotteiden hankinnassa ja käytössä.

Asiasanat: Älylukko, Tietoturva, IoT, OSI-malli

Sisällys

Kuvat

Taulukot

1 Johdanto

Älylukkojen käyttö on yleistynyt merkittävästi kodin turvallisuusratkaisuina. Älylukot ovat monipuolisia laitteita, jotka hyödyntävät eri OSI-mallin kerroksia tarjotakseen laajan valikoiman toiminnallisuuksia ja palveluita. Fyysinen kerros käsittää kaikki laitteistoon liittyvät näkökohdat, kuten langattomat tai fyysiset yhteydet älylukon ja verkon välillä. Siirtokerros tarjoaa keinoja varmistaa virheetön tiedonsiirto älylukon ja verkon välillä. Protokollat kuten Bluetooth Low Energy (BLE) tai Zigbee voivat olla osa tätä kerrosta, tarjoten luotettavan viestintäkanavan älylukkojen ja verkon välillä. Sovelluskerroksessa älylukot voivat käyttää erilaisia protokollia, kuten HTTP tai MQTT, verkkoon liittymiseen ja tiedonsiirtoon. Tässä kerroksessa hoidetaan sovellustason palveluita, kuten käyttöoikeuksien hallintaa ja lokitietojen siirtoa älylukoilta verkkoon.[1]

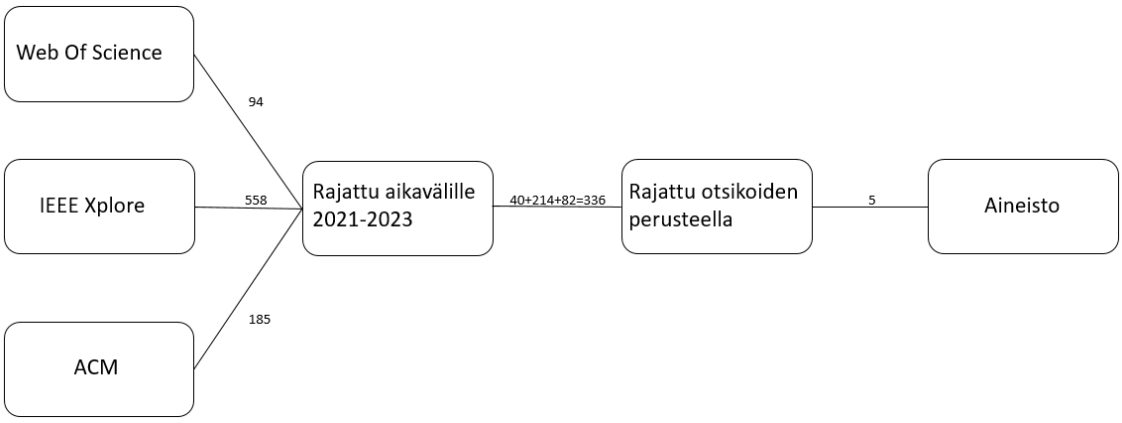
Tämän tutkielman tarkoituksena on tarkastella älylukkoihin liittyviä tietoturvia sekä pohtia mahdollisia suojauskeinoja tietoturvan parantamiseksi. Tässä tutkielmassa on kaksi tutkimuskysymystä:

- Tk1: Mitkä ovat älylukkojen tietoturvariskit?
- Tk2: Millaisia käytännön suojauskeinoja voidaan soveltaa älylukkojen tietoturvan parantamiseksi?

Älylukkojen käyttö on yleistynyt merkittävästi kodin turvallisuusratkaisuina. Tässä tutkielmassa tarkastellaan Yale ja iLOQ -älylukkojen ominaisuuksia ja vertaillaan niiden tarjoamia turvatoimintoja. Vaikka älylukkojen sovellusalueet voivat olla

laajat, tässä tekstissä keskitytään nimenomaisesti älykotien ovilukkoihin ja niiden tietoturvaan.

Tutkielman ensimmäisessä vaiheessa suoritettiin lähteiden haku seuraavista tietokannoista: IEEE, Web of Science ja ACM. Hakulauseena käytettiin "(privacy OR security) AND 'smart lock*','mikä tuotti yli tuhat tulosta. Tämän tietomäärän käsittelyn helpottamiseksi asetettiin aikaraja, joka rajoitti julkaisuvuodet vuosien 2021 ja 2023 välille. Rajauksen jälkeen Web of Science -tietokannasta löytyi 40 artikkelia, IEEE Xploresta 214 ja ACM:stä 82. Näistä artikkeleista suoritettiin lisärajaus otsikoiden perusteella. Lopulta valittiin tutkielman aineistoksi 5 artikkelia. Valitsin tutkielmani vertailukohteiksi Yale ja iLOQ -älylukot. Hakuprosessi on havainnollistettu kuvassa 1.1.



Kuva 1.1: Aineistohaun vaiheet

Tutkielma koostuu kahdesta pääluvusta johdannon lisäksi. Toinen luku käsittelee älylukkoja ja OSI-mallia ja kolmas luku tarkastelee eri laitevalmistajien tarjoamia älylukkoratkaisuja tietoturvallisuuden näkökulmasta.

Toisessa luvussa esitellään älylukkojen käyttömahdollisuuksia, keskittyen erityisesti eri valmistajien älylukkoihin ja OSI-malliin. Luku esittelee yleisesti älylukkojen merkityksen ja käytön eri ympäristöissä. Siinä kerrotaan älylukkojen digitaalisen

teknologian hyödyt ja lisäominaisuudet, kuten etäohjauksen ja älykkäät käyttäjätunnistusratkaisut. Toisessa luvussa esitellään valitut älylukot, Yale ja iLOQ, ja niiden taustat. Toisessa luvussa esitellään valittujen älylukkojen mallit sekä niiden tarjoamat ominaiuudet.

Kolmas luku käsittelee älylukkojen tietoturvaa. Aluksi tarkastellaan yleisesti tietoturvaa ja sen jälkeen syvennytään älylukkojen tietoturvaan. Luvussa analysoidaan älylukkojen tietoturvariskejä OSI-viitemallin kerroksittain. Tietoturvariskien esittelyn jälkeen esitetään erilaisia keinoja riskien minimoimiseksi, jälleen OSI-viitemallin kerroksia hyödyntäen. Lisäksi luvussa käsitellään tietoturvaratkaisujen toteuttamisen haasteita. Tutkielman loppuosassa käsitellään älylukkojen tietoturvaa ja siihen liittyviä riskejä, kuten jamming-hyökkäyksiä ja unenpuutteen hyökkäyksiä. Keskitason tietoturvauhat liittyvät verkko- ja siirtokerroksiin. Tutkielma viittaa myös IoT-alustojen turvallisuuteen ja suosittelee monimutkaista salausmenetelmää päästä-päähän-tietoturvaan.

Neljännessä ja viimeisessä luvussa tehdään tutkielman tuloksista johtopäätökset ja kootaan tutkielman keskeiset asiat yhteen kokonaisuuteen.

2 Kodin älylukot

2.1 Eri valmistajien älylukot

Älylukot muodostavat nykyaikaisen turvallisuusjärjestelmien kehittyneen osan, tarjoten käyttäjille monipuolisia ja älykkäitä toimintoja. Näitä lukkoja käytetään laajalti erilaisissa ympäristöissä, kuten kotitalouksissa, yrityksissä ja julkisissa tiloissa. Älylukot eroavat perinteisistä lukkomekanismeista siinä, että ne hyödyntävät digitaalista teknologiaa tarjotakseen turvallisempaa ja helppokäyttöisempää pääsyä sekä lisäominaisuuksia, kuten etäohjausta ja älykkäitä käyttäjätunnistusratkaisuja. Valitsin tutkielmani vertailukohteiksi Yale ja iLOQ -älylukot. Yale ja iLOQ ovat molemmat tunnettuja älylukkoteknologian valmistajia, joilla on vahva historia ja innovatiivisia lähestymistapoja turvallisuuden alalla. Vertailtaessa näitä kahta valmistajaa ja heidän älylukkoratkaisujaan, on tärkeää tarkastella niiden taustaa, tarjoamia tuotteita sekä teknisiä ominaisuuksia.

Yalen tarina sai alkunsa 1840-luvulla Linus Yalen visionäärisestä päätöksestä perustaa liike, jonka pääasiallinen tarkoitus oli myydä lukkoja pankkien käyttöön. Ensimmäisen liikkeensä avaamisen jälkeen Yale laajensi toimintaansa perustamalla tehtaan Newportiin Yhdysvaltoihin. Linus Yale Seniorin johtama pieni lukkotehdas kasvoi ajan myötä Yale & Towne Companyn perustamiseen Connecticutin Stanfordiin yhteistyössä Linus Yale Juniorin ja Henry Townen kanssa. 1900-luvun alussa Yale & Towne Company oli vakiinnuttanut asemansa maailmanlaajuisesti, työllis-

täen yli 12 000 henkilöä ja nousten johtavaksi toimijaksi lukitusalalla. Vuonna 2000 ASSA ABLOY Group, maailman johtava lukituskonserni, hankki Yalen vahvistaen entisestään sen asemaa turvallisuusalalla. Yalen sitoutuminen turvallisuuden kehittämiseen konkretisoitui vuonna 2016, kun yritys laajensi tuotevalikoimaansa älykkäillä turvalaitteilla, kuten hälyttimillä ja kameroilla. Näiden innovaatioiden avulla käyttäjät voivat helposti valvoa kodin ja läheistensä turvallisuutta kätevien sovellusten avulla, sijainnista riippumatta. Tämä kehitys kuvastaa Yalen jatkuvaa pyrkimystä tarjota asiakkailleen luotettavia turvaratkaisuja. [2] Yale on ASSA ABLOY -konsernin osa, joka on maailman johtava kulkuratkaisujen toimittaja. Suomessa Yalea edustaa Abloy Oy. Älylukkojen yhteydessä käytetään Secured by ABLOY -leimaa. Lukkojen toimivuus, turvallisuus ja laatu testataan samoilla standardeilla kuin muidenkin ABLOY-tuotteiden. [3]

Yalen älylukkoperheeseen kuuluu kolme erilaista mallia: Doorman L3, Doorman V2N ja Linus. Yale Doorman tarjoaa käyttäjille modernin lukkoratkaisun, joka mahdollistaa kodin lukituksen avaamisen koodilla, kulkutunnisteella tai älypuhelimella. Yale hyödyntää älylukkojensa hallintaan Yale Home -sovellusta sekä Yale Connect Wi-Fi Bridge -lisälaitetta. Sovellus tarjoaa käyttäjille mahdollisuuden hallinnoida älylukkojaan ja muita tulevia Yale-turvatuotteita yhdellä yhtenäisellä alustalla.[4] Yale Connect Wi-Fi Bridge -lisälaite on osa älykodin kehittyvää ekosysteemiä, joka tarjoaa tavan hallita Yale-älylukkoja etänä ja integroida ne ääniavustajien kautta älykotijärjestelmiin. Laite toimii siltana älylukon ja kodin langattoman verkon välillä, mahdollistaen käyttäjälle etäavaukset ja reaaliaikaisen seurannan. Laitteen tekniset ominaisuudet, kuten Bluetooth 4.0 -yhteystekniikka ja 2.4 GHz Wi-Fi.[5]

iLOQ on suomalainen yritys, joka on erikoistunut muuttamaan perinteisen mekaanisen lukituksen digitaaliseksi pääsyoikeuksien hallinnaksi. iLOQ on perustettu vuonna 2003. Yksi iLOQin merkittävistä saavutuksista oli vuonna 2007 markkinoille tuotu maailman ensimmäinen elektroninen lukitusjärjestelmä. Järjestelmässä lukkosylinterit saavat tarvitsemansa sähköenergian avaimen työntöliikkeestä, mikä tekee pääsyoikeuksien hallinnasta digitaalisella iLOQilla helppoa ja turvallista. Tämä ratkaisu ei vaadi paristoja tai kaapeleita. Vuonna 2016 iLOQ esitteli iLOQ S50 -tuoteperheen, vahvistaen asemaansa omavoimaisen lukituksen edelläkävijänä. iLOQ S50 on pääsynhallintajärjestelmä, jonka lukkosylinterit keräävät tarvitsemansa sähkövirran NFC-puhelimesta. Tämä ratkaisu toimii avaimena ja virtalähteenä ilman tarvetta paristoille tai kaapeleille, soveltuen erityisesti hajautettuihin sarjalukostoihin. Vuonna 2019 iLOQ esitteli iLOQ S5:n, joka hyödyntää digitalisaation ja esineiden internetin mahdollisuuksia. Käyttäen iLOQ S10:n toimintavarmaa mekaniikkaa ja uutta elektroniikkaa, iLOQ S5 tarjoaa lisäarvoa käyttäjilleen, tarjoten tietoturvan, käyttöoikeuksien hallinnan ja elinkaarikustannukset. Vuonna 2020 iLOQ esitteli iLOQ 5 Series -alustan, suunnitellun turvallisuuden, minimoimisen ylläpitoaikaa ja ympäristövaikutuksia, pienentämään elinkaarikustannuksia ja lisäämään kiinteistöjen arvoa. iLOQ 5 Series hallinnoi useita lukitusjärjestelmiä, tarjoten yhtenäisen ratkaisun eri pääsynhallinnan tarpeisiin. Vuonna 2022 iLOQ esitteli iLOQ HOME -laajennuksen, joka liittyy iLOQ 5 -lukitusjärjestelmään ja iLOQ 5 Series -alustaan. iLOQ HOME on pääsynhallintajärjestelmä, joka tarjoaa vapautta, turvallisuutta ja joustavuutta, poistaen perinteisten lukitusjärjestelmien rajoitukset.[6]

Molemmat valmistajat tarjoavat älykkäitä ominaisuuksia, kuten etäkäyttöä ja monipuolisia avainvaihtoehtoja. Yalen älylukot, kuten Doorman L3, korostavat turvallisuutta ja helppokäyttöisyyttä erilaisissa olosuhteissa. iLOQ puolestaan tuo esille omavoimaiset teknologiat, jotka keräävät tarvitsemansa sähkövirran NFC-puhelimesta ilman paristoja tai kaapeleita. Yhteenvetona voidaan todeta, että sekä

Yale että iLOQ ovat oman alansa edelläkävijöitä tarjoten älykkäitä lukkoratkaisuja, joilla on vahvat tekniset ominaisuudet ja kyky sopeutua erilaisiin käyttötilanteisiin. Valinta näiden kahden välillä riippuu käyttäjän tarpeista ja painotuksista, kuten käytön helppoudesta, turvallisuudesta ja mahdollisuuksista integroitua laajempiin älykotijärjestelmiin. Yalen vahvuuksiin kuuluu pitkä historia lukkoteollisuuden parissa ja sitoutuminen jatkuvaan innovointiin. Yalen älylukot, kuten Doorman L3, ovat tunnettuja modernista muotoilusta ja monipuolisista turvallisuusominaisuuksista. Yale on myös osa ASSA ABLOY -konsernia, maailman johtavaa kulkuratkaisujen toimittajaa, mikä lisää sen uskottavuutta ja asiantuntemusta turvallisuusalalla. iLOQ taas erottuu omavoimaisen lukitusteknologian edelläkävijänä. iLOQin älylukot tarjoavat paristottoman ja kestävän vaihtoehdon perinteisille lukitusjärjestelmille. Tämä on erityisen hyödyllistä hajautetuissa sarjalukostoissa, missä perinteiset paristokäyttöiset ratkaisut voivat olla haastavia ylläpidon ja kustannusten suhteen.[7] Taulukossa 2.1 on esiteltynä älylukkojen ja niiden hallintajärjestelmien teknisiä ominaisuuksia.

Malli	Toiminnot	Tekniset ominaisuudet	Hallinta
Yale Doorman L3	Avaimeton lukitus koodilla, älypuhelimella, kulkutunnisteella	IP55-luokitus, käyttölämpötilat, pariston kesto	Yale Home -mobiilisovellus, Yale Connect Wi-Fi Bridge
Yale Doorman V2N	Avaimeton pääsy koodilla, kulkutunnisteella, kaukoavaimella, älypuhelimella	sisäänrakennettu hälytin	Yale Home -mobiilisovellus, Yale Access -lukkomoduuli
Yale Linus	Avaimeton pääsy älypuhelimella tai perinteisellä avaimella, automaattinen avaustoiminto	Bluetooth 2.4GHz (Versio 4.2), kaksivaiheinen varmennus, AES- ja TLS-salaukset	Yale Home -mobiilisovellus, Yale Connect Wi-Fi Bridge
iLOQ HOME	Tarkka avaintenhallinta, kadonneiden avainten välitön poistaminen, etäyhteys asuntoon	NFC-yhteys, pääsykoodin jakaminen, pilvipohjainen ohjelmisto	NFC-yhteydellä varustettu älypuhelin
iLOQ S5	Omavoimainen sähkömekaaninen lukkosylinteri, ohjelmoitava, EN 15684 ja SSF-sertifikaatit	Ohjelmointi iLOQ P55S.1 -ohjelmointiavaimella, Bluetooth 2.4GHz	iLOQ P55S.1 -ohjelmointiavain, iLOQ D2D-verkko
iLOQ S50	Paristoton sähkömekaaninen lukkosylinteri, NFC-virtalähde, AES256-salaus	Ensiohjelmointi tietokoneella, iLOQ P55S.1 -ohjelmointiavain	NFC-yhteydellä varustetut Android- ja iOS-puhelimet, iLOQ K55S -avain
iLOQ 5-series	Omavoimainen digitaalinen lukitusjärjestelmä, NFC-virroitettu, pilvipohjainen ohjelmisto	Älypuhelimen käyttö avaimena ja virtalähteenä, AES256-salaus	Monipuoliset avainvaihtoehdot, reaaliaikainen pääsyoikeuksien hallinta

Taulukko 2.1: Älylukkojen teknisiä ominaisuuksia [4] [7]

2.2 OSI-viitemalli

OSI-viitemalli on verkkomalli, joka koostuu seitsemästä kerroksesta. OSI-viitemalli kuvaa tietoliikennettä eri tasoilla aina fyysisestä komponentista sovellustasolle saakka. OSI-mallin kerrokset perustuvat useisiin keskeisiin periaatteisiin, jotka ohjaavat niiden suunnittelua ja toimintaa. Ensinnäkin kerros tulisi luoda aina, kun tarvitaan erilaista abstraktiota. Jokaiselle kerrokselle on asetettava selkeästi määritelty tehtävä ja niiden tulisi suorittaa tiettyä toimintoa tai tarjota tietty palvelutaso. Jokaisen kerroksen tehtävän valinnassa on otettava huomioon kansainvälisesti standardoidut protokollat ja kerrosrajat tulisi valita siten, että tietovirta rajapintojen yli minimoidaan. Kerrosten lukumäärän tulisi olla riittävän suuri, jotta erillisiä toimintoja ei tarvitse sijoittaa väkisin samaan kerrokseen. Näitä kerroksia ovat fyysinen kerros (physical layer), siirtokerros (data link layer), verkkokerros (network layer), kuljetuskerros (transport layer), istuntokerros (session layer), esitystapakerros (presentation layer) ja sovelluskerros (application layer). [8] OSI-viitemallin kerrokset havainnollistettuna kuvassa 2.1.

Kuva 2.1: OSI-viitemallin kerrokset [9]

Fyysisellä kerroksella keskitytään raakadatan siirtämiseen viestintäkanavan yli. Suunnittelukysymykset liittyvät siihen, että varmistetaan, että toisen osapuolen lähettäessä 1-bitin, se vastaanotetaan toisen osapuolen toimesta 1-bittinä eikä 0-bittinä. Tässä yhteydessä pohditaan muun muassa, mitä sähköisiä signaaleja tulisi käyttää 1:n ja 0:n edustamiseen, kuinka pitkä aika yksi bitti kestää, voiko tiedonsiirto tapahtua samanaikaisesti molempiin suuntiin, miten alustava yhteys muodostetaan, kuinka se suljetaan molempien osapuolten ollessa valmiita.[8]

Siirtokerroksen päätehtävä on muuntaa raaka siirtoyhteys virheettömän näköiseksi linjaksi, jossa ei ole havaittuja siirtohäiriöitä. Se tekee niin peittämällä todelliset virheet, jotta verkko ei havaitse niitä. Tämä tehtävä suoritetaan siten, että lähettäjä pilkkoo syöteaineiston datarungoiksi ja lähettää rungot peräkkäin. Jos palvelu on luotettava, vastaanotin vahvistaa kunkin rungon oikean vastaanoton lähettämällä takaisin vahvistuskehyksen. Siirtokerros voi tarjota keinoja varmistaa virheetön tiedonsiirto älylukon ja verkon välillä. [8] Protokollat kuten Bluetooth Low Energy (BLE) tai Zigbee voivat olla osa tätä kerrosta. Bluetooth Low Energy (BLE) on standardi lyhyen matkan langattomalle viestinnälle, jonka on määritellyt Bluetooth SIG (Special Interest Group). Se toimii ISM 2,4 GHz -kaistalla ja toimii ad-hoc-pistekohtaisena PAN-tekniikkana. Radiokommunikaatio perustuu taajuushyppely-leviämisspektriin (FHSS) varattujen taajuuksien välttämiseksi. Tällä tekniikalla se tarjoaa jopa 1 Mb/s yli 1 MHz:n kanavien. [1]

Verkkokerros ohjaa aliverkon toimintaa ja ylläpitää palvelun laatua. Olennainen suunnittelukysymys on, miten paketit ohjataan lähteestä määränpäähän. Reititys voi perustua staattisiin taulukoihin, jotka ovat verkkoon "sisäänrakennettuja"eivätkä muutu usein, tai vaihtoehtoisesti ne voidaan päivittää automaattisesti välttääkseen vikaantuneet komponentit. Reititys voidaan myös määrittää jokaisen keskustelun alussa, kuten esimerkiksi etäkoneeseen kirjautumisen yhteydessä. voivat olla erittäin dynaamisia, määrittyen uudelleen jokaiselle paketille heijastaakseen

nykyistä verkkokuormaa. Jos liian monta pakettia on läsnä aliverkossa samanaikaisesti, ne voivat mennä toistensa tielle ja muodostaa tukkeumia. [8] Verkkokerros huolehtii datan luotettavasta siirrosta aistikerroksesta, sen alkuperäisestä käsittelystä rajoitetuissa laitteissa tai porteissa, oikeasta luokittelusta sekä datan muodon muuttamisesta. Se käsittää datan vaihdon eri verkkojen välillä, kuten paikallinen verkko, pääsyverkko (kiinteä, langaton - matkapuhelinverkko) ja ydinverkko. [1]

Kuljetuskerroksen tehtävänä on vastaanottaa data yläpuolelta, tarvittaessa jakaa se pienempiin yksiköihin, välittää ne verkkokerrokselle ja varmistaa, että palaset saapuvat oikein toiseen päähän. Lisäksi kaiken tämän on tapahduttava tehokkaasti ja tavalla, joka eristää yläkerrokset ajasta riippuvien muutosten suhteen laitteistoteknologiassa. Kuljetuskerros määrittää myös, millaista palvelua tarjotaan istuntokerrokselle ja lopulta verkon käyttäjille. Yleisin kuljetusyhteyden tyyppi on virheetön pisteestä pisteeseen -kanava, joka toimittaa viestit tai tavut niiden lähetys järjestyksessä. Kuitenkin muita mahdollisia kuljetusyhteyden palvelutyyppejä on olemassa, kuten eristettyjen viestien kuljettaminen ilman takuuta toimitusjärjestyksestä ja viestien lähettäminen useisiin kohteisiin.[8]

Istuntokerros mahdollistaa käyttäjille eri koneilla istuntojen muodostamisen keskenään. Istunnot tarjoavat erilaisia palveluita, kuten vuoropuhelun hallinnan, joka seuraa kenen vuoro on lähettää, tokenien hallinnan, joka estää kahden osapuolen yrittämisen samaa kriittistä toimenpidettä samanaikaisesti, sekä synkronoinnin. Synkronointi mahdollistaa pitkien siirtojen tarkastuspisteet, mikä sallii niiden jatkamisen siitä, mihin ne jäivät mahdollisen kaatumisen ja seuraavan palautumisen tapauksessa.[8]

Esitystapakerros käsittelee siirrettävän tiedon syntaksia ja semantiikkaa. Tietokoneiden, joilla on erilaiset sisäiset tietoesitykset, välistä viestintää varten vaihdettavat tietorakenteet voidaan määritellä abstraktilla tavalla, yhdessä standardoidun koodauksen kanssa, jota käytetään tiedonsiirrossa. Esitystapakerros hallinnoi näi-

tä abstrakteja tietorakenteita ja mahdollistaa korkeamman tason tietorakenteiden määrittämisen ja vaihtamisen. [8]

Sovelluskerros sisältää joukon protokollia, joita käyttäjät yleisesti tarvitsevat. Yksi laajalti käytetty sovellusprotokolla on HTTP (HyperText Transfer Protocol), joka on perusta World Wide Webille. Kun selain haluaa verkkosivun, se lähettää HTTP:n avulla sivun nimen palvelimelle, joka isännöi sivua. Palvelin lähettää sitten sivun takaisin. Sovelluskerroksen osalta älylukot voivat käyttää erilaisia protokollia, kuten HTTP tai MQTT, verkkoon liittymiseen ja tiedonsiirtoon sovellustason palveluiden, kuten käyttöoikeuksien hallinnan ja lokitietojen lähetysten, kautta. [8] Sovelluskerros tarjoaa yksilöllisiä palveluita käyttäjän tarpeiden mukaisesti. Jotskus erotetaan ylimääräinen kerros, jota kutsutaan tukikerrokseksi. Tämä kerros on suunniteltu luomaan tukialusta sovelluskerrokselle, erityisesti IoT-datan valmistelussa ja järjestämisessä. Tässä kontekstissa tukikerros olisi vastuussa datan laskennasta, kokoamisesta ja saattamisesta sovelluskerroksen saataville. [1]

3 Älylukkojen tietoturva

3.1 Tietoturva

Älykodin infrastruktuurin yleiset turvallisuusvaatimukset kattavat kuusi tunnettua tavoitetta: luottamuksellisuus/yksityisyys, eheys, aitous, kiistämättömyys, saatavuus ja valtuutus. Kuitenkin toisin kuin internetiin kytketyillä päätelaitteilla, useimmilla älykotilaitteilla ei ole yhtenäistä suoritusympäristöä eikä riittävästi laskentatehoa. Tämän vuoksi monimutkaisen turvallisuusstrategian toteuttaminen on haastavaa. Koska älykotiympäristö perii osittain komponenttejaan esineiden internetin (IoT) järjestelmistä, jotkin turvallisuuteen liittyvät luokat, jotka kuvaavat IoT-alustoja, voidaan soveltaa myös älykoteihin, erityisesti langattomien anturiverkkojen osalta.

3.2 Tietoturvariskit

Älykodit tuovat mukanaan myös fyysistä vaaraa, kuten älylukon manipulointia asuntoon murtautumiseksi.[10] Useissa tarkastuksissa älykkäissä yhteyksissä olevien laitteiden osalta on tunnistettu laaja kirjo tietoturvauhkia ja hyökkäyksiä, jotka kohdistuvat esineiden internetin (IoT) laitteisiin. Näitä tietoturvauhkia voidaan systematisoida IoT:n eri kerrosten näkökulmasta. Matalan tason tietoturvauhat liittyvät fyysiseen ja datalink-kerrokseen sekä laitteiston tasolle. Näihin sisältyvät esimerkiksi jamming-hyökkäykset, joissa vastustaja voi suorittaa erilaisia palvelunestohyök-

käyksiä, sekä turvattoman alustuksen riski, jossa fyysisen kerroksen viestintää on suojattava asianmukaisella alustuksen ja konfiguroinnin mekanismilla. Matalan tason Sybil-hyökkäykset ja turvattoman fyysisen liitännän mahdollisuus muodostavat myös merkittäviä uhkia verkon eheydelle. Unenpuutteen hyökkäys puolestaan on erityisen vaarallinen, sillä sen tavoitteena on maksimoida anturisolujen virrankulutus minimoidakseen niiden eliniän.[11]

Keskitason tietoturvauhat kohdistuvat verkko- ja siirtokerroksiin. Esimerkkejä näistä uhkista ovat uudelleentoistohyökkäykset tai duplikaatit fragmentoinnin vuoksi, RPL-reitityshyökkäykset sekä todennus ja turvallinen viestintä, jotka muodostavat keskeisen osan laitteiden ja käyttäjien tietoturvaa IoT:ssa. Myös siirtotason päätä-päähän-tietoturvaan liittyy keskitason uhkia, ja suositeltavaa on käyttää mahdollisimman monimutkaista salausmenetelmää varmistaakseen viestinnän turvallisuuden.[11]

Korkean tason tietoturvauhat keskittyvät sovelluskerrokseen. Näitä ovat esimerkiksi CoAP-tietoturva internetissä, joka voi altistua erilaisille hyökkäyksille, turvattomat rajapinnat, jotka voivat aiheuttaa riskin datan saavutettavuudelle, sekä turvaton ohjelmisto/firmware, joka altistuu useille haavoittuvuuksille. Väliohjelmiston tietoturva on myös keskeinen tekijä mahdollistamassa viestintää kaikkien IoT:n osien välillä. Lisäksi pilvihyökkäykset muodostavat kasvavan uhan älykotijärjestelmille, ja niiden vaikutus voi olla merkittävä eri pilvipalvelumalleja vastaan. SQL-injektiot, mies keskellä -hyökkäykset, sniffaushyökkäykset ja palvelunestohyökkäykset ovat esimerkkejä pilviuhkista, jotka voivat tehdä palveluista saavuttamattomia tarkoitetuille käyttäjille. Tämän vuoksi on korostettava tietoturvan merkitystä kaikilla tasoilla varmistaakseen älykkäiden laitteiden ja järjestelmien luotettavuus ja turvallisuus.[11]

Verkkokerroksen tietoturvariskit voivat kohdistua monenlaisiin uhkiin, jotka voivat vaarantaa älykotien turvallisuuden ja toimivuuden. Näitä uhkia ovat muun muas-

sa haitallisen koodin suorittaminen verkkoyhteyden kautta, palvelunestohyökkäykset, luvaton pääsy paikallisiin verkkoresursseihin, internet-yhteyteen vaikuttavat katkokset ja internet-yhteyteen vaikuttavat häiriöt.[1]

Haitallisen koodin suorittaminen verkkoyhteyden kautta mahdollistaa täydellisen tai osittaisen etäohjauksen laitteista. Tämä vaihtelee yksittäisten laitteiden etäkomentojen suorittamisesta aina älykkäiden laitteiden verkostojen järjestämiseen tietyn toiminnon suorittamiseksi. Keskeiset uhat, jotka liittyvät rajoitettujen laitteiden käyttöön älykotiympäristössä, kohdistuvat niiden alttiuteen DoS-hyökkäyksille. Tällaiset hyökkäykset voivat nopeasti johtaa rajoitetun solmun resurssien ehtymiseen, koska rajoitetut suoritin- ja muistiresurssit tekevät laitteista haavoittuvia resurssien ehtymiselle. Tämä luo mahdollisuuden hyökkääjälle lähettää jatkuvia pyyntöjä, jotka käsitellään tietyissä solmuissa, aiheuttaen resurssien ylikäyttöä. Seurauksena radiokanavat ruuhkautuvat, mikä lopulta voi johtaa älykkäiden laitteiden välisen viestinnän kanavien sulkemiseen.[1]

Luvaton pääsy paikallisiin verkkoresursseihin mahdollistaa pääsyn HAN-yhteydessä oleviin laitteisiin, erityisesti niiden asetuksiin, jotka voivat vaikuttaa verkkoviestintään. Open Web Application Security Project (OWASP) on kuvannut tämän uhkaryhmän seuraavasti: Epävarmat verkkopalvelut voivat mahdollistaa HAN-yhteydessä olevien laitteiden kytkemisen pois päältä. Turvattomat ohjelmistot/firmware voivat antaa hyökkääjälle mahdollisuuden suorittaa oma haitallinen päivitys, esimerkiksi DNS-kaappausten avulla. Kuljetuksen salaamisen ja eheyden varmistuksen puuttuminen voi johtaa tietoliikenteen salakuunteluun HAN-yhteydessä siirrettävissä tiedoissa. Yllä mainitut uhat sisältävät myös huonosti suojatut päästä päähän -kuljetuspalvelut, jotka on toteutettu joissakin älylaitteissa. OWASP korostaa myös tietoturvavikoja hallintatoiminnoissa, erityisesti verkkosovellusten tietoturvassa.[1]

Internet-yhteyteen vaikuttavat katkokset laajentavat aistikerroksen määriteltyjä tapauksia ja viittaavat Internetin kautta saatavilla oleviin resursseihin. Esimerkilliset hyökkäykset voivat aiheuttaa Internet-yhteyden katkoksen, mikä on välttämätöntä joillekin älykotisovelluksille. [1]

Sovelluskerroksen tietoturvariskeissä käsitellään useita uhkia, jotka voivat vaikuttaa älykotipalveluiden turvallisuuteen. Näihin kuuluvat älykotipalvelun estäminen, luottamuksellisen tiedon kompromissointi ja henkilötietojen väärinkäyttö, luvaton pääsy tietojärjestelmiin ja laitteiden hallinnan luvaton käyttö ja valtuuksien väärinkäyttö, palvelukatkokset sekä IT-varojen vahingoittuminen. Älykotipalvelun estäminen tapahtuu sovelluskerroksella, missä DoS-hyökkäykset voivat kohdistua älykotiratkaisun tarjoajan käyttämiin erityispalveluihin, esimerkiksi uusien laitteiden rekisteröintiin. Tämä voi johtaa palvelimien ylikuormittumiseen. [1]

Luottamuksellisen tiedon kompromissointi ja henkilötietojen väärinkäyttö liittyvät pilvipalveluntarjoajiin ja IoT-ratkaisujen tarjoajiin, jotka tallentavat älykotisovellusten käyttäjien dataa. Pilvipalveluntarjoajia pidetään luotettavina, mutta sisäpiirin hyökkäykset voivat altistaa tallennetut tiedot väärinkäytölle, kuten yksityisyyden loukkauksille tai laajamittaisille tietomurroille. Luvaton pääsy tietojärjestelmiin ja laitteiden hallinnan luvaton käyttö ja valtuuksien väärinkäyttö liittyvät pääsyyn hallintotehtäviin, ja ne ovat kriittisiä verkkosovellusten tietoturvan kannalta. OWASP on korostanut alueen puutteita, kuten turvatonta verkkokäyttöliittymää, riittämätöntä todennusta/valtuutusta ja henkilötietojen puutteellista suojausta.[1]

Palvelukatkokset ja IT-varojen vahingoittuminen laajentavat tapauksia, jotka on määritelty havaintokerrokselle ja verkkokerrokselle. Tämä uhkaryhmä viittaa palvelukohtaisiin resursseihin, jotka ovat saavutettavissa Internetin kautta, ja ne voivat aiheuttaa älykotisovellusten toimintahäiriöitä, esimerkiksi laitetoimittajan tukipalvelimien saatavuuden puuttuessa.[1]

Taulukossa 3.1 on esimerkkeinä älylukkojen tietoturvariskeistä sekä niille mahdollisia ratkaisuja, joilla estää tietoturvauhat.

Tietoturvariski	Ratkaisuesimerkki
Etäohjausriskit	Käytä vahvaa salausprotokollaa ja monivaiheista käyttäjän vahvistusta suojatakseen etäohjauksen.
Heikko salaus	Käytä vahvaa salaustekniikkaa, kuten AES, parantamaan älylukon tietoturvaa.
Fyysinen manipulaatio	Käytä vahvoja rakennusmateriaaleja ja fyysisiä turvatoimia torjumaan hyökkäyksiä.
Ohjelmistopäivitysten laiminlyönti	Tarkista säännöllisesti ja päivitä älylukon ohjelmisto automaattisesti haavoittuvuuksien minimoimiseksi.
Yhteysprotokollat	Käytä turvallisia ja vahvistettuja yhteysprotokollia, kuten Bluetooth 4.0 tai uudempaa.
Käyttäjätunnusten hallinta	Vaadi vahvat salasanat ja käytä monivaiheista vahvistusta käyttäjien tunnistamiseksi.
Pilvipalvelun turvallisuus	Käytä turvallista pilvipalveluntarjoajaa ja vahvista kommunikaatio älylukon ja pilven välillä.
Yksityisyysriskit	Tarjoa käyttäjille selkeät hallintamahdollisuudet omasta datastaan ja noudata tietosuojakäytäntöjä.

Taulukko 3.1: Taulukko tietoturvariskeistä [1][11]

3.3 Tietoturvan suojauskeinot

Yale on omalta osaltaan sitoutunut varmistamaan käyttäjien tietoturvan. Yhtiö säilyttää henkilötietoja niin kauan kuin ne ovat tarpeellisia kerättyjen tietojen tarkoitukseen. Käyttäjillä on oikeus pyytää pääsyä henkilötietoihinsa, oikaista virheelliset tiedot, ja heillä on oikeus tietojen poistamiseen tietyissä tilanteissa. äyttäjille annetaan myös oikeus vastustaa henkilötietojensa käsittelyä ja pyytää tietojen käsittelyn rajoittamista tietyissä tilanteissa.[12]

Yale-älylukot ovat Abloy Secured -sertifioituja, mikä tarkoittaa, että ne läpäisevät samat tiukat turvallisuus-, laatu- ja käyttökokemustestit kuin muut Abloyn lukitusratkaisut. Yale Doorman V2N ja Yale Doorman L3 -älylukoissa on integroi-

tu murtohälytin, joka reagoi mahdollisiin murtoyrityksiin. Hälytin voi käyttää sekä äänimerkkiä että sireenihälytystä, erityisesti silloin, kun älylukko on integroitu hälytysjärjestelmään. Mobiililaitteeseen liitetty älylukko lähettää myös omistajalle ilmoituksen mahdollisesta murtoyrityksestä, toimien tehokkaana pelotteena tunkeutujille. Automaattinen lukintatoiminto varmistaa, että älylukko-ovi sulkeutuu automaattisesti, välttäen inhimillisten virheiden aiheuttamat riskit.

Yale Doorman ja Yale Linus -älylukot on suunniteltu lukittumaan automaattisesti oven sulkeuduttua. Lisäksi etäohjauksen mahdollistava Yale Connect Wifi Bridge -lisäosa mahdollistaa lukituksen tilan tarkistamisen etänä, mikä lisää käyttäjän hallintaa ja turvallisuutta. Avaimettoman älylukon käyttö eliminoi perinteisiin avaimiin liittyviä riskejä, kuten kadonneiden tai unohtuneiden avainten aiheuttamia haasteita. Älylukko tarjoaa käyttäjälle mahdollisuuden hallita kulunvalvontaa helposti ja turvallisesti, poistaen huolen varavaihtoehtojen, kuten vara-avainten, käyttämisestä. Kulunseuranta on yksi älylukon merkittävistä eduista. Yale Home -sovelluksen avulla käyttäjä voi tarkistaa älylukon tilan ja kulkua helposti, mahdollistaen ovensa valvonnan etänä. Mobiilisovellus mahdollistaa myös käyttölokin seuraamisen, jolloin omistaja voi nähdä, kuka ja milloin on avannut oven. Tämä lisää merkittävästi turvallisuutta ja tuo käyttäjälle arvokasta tietoa asunnon tapahtumista. Älylukkojen käyttäjät voivat omalta osaltaan varmistaa laitteidensa turvallisuuden. Säännölliset laiteohjelmiston päivitykset, mobiilisovelluspäivitysten ylläpito ja kodin internetyhteyden suojaaminen vahvalla salasanalla ovat suositeltavia käytäntöjä. Yale Home -sovelluksen kaksivaiheinen tunnistautuminen ja mahdollisuus poistaa sovellus ja virtuaaliset avaimet kadonneen puhelimen tapauksessa lisäävät entisestään älylukon käyttöturvallisuutta.[13]

BLE:llä on oma salausmenetelmänsä, tämä protokolla luottaa pääasiassa omaan AES256-salaukseen, sekä lisäämään turvallisuutta että helpottamaan lisäominai-

suuksia. AES256 on symmetrinen salausmenetelmä, joka vaatii jaetun 256-bittisen avaimen sekä viestin salaamiseen että purkamiseen.[14]

Taulukkoon 3.2 on taulukoituna älylukkojen tietoturvaominaisuuksia ja mitä kuluttajat voivat mahdollisesti ymmärtää ja ottaa huomioon hankkiessaan älylukkoja.

Älylukon tietoturvaominaisuus	Mitä asiakkaan tulisi ymmärtää
Vahva salasanasuojaus	Valitse ainutlaatuinen ja monimutkainen salasana. Käytä monivaiheista vahvistusta, kun mahdollista.
Ohjelmistopäivitysten tärkeys	Säännölliset päivitykset ovat välttämättömiä haavoittuvuuksien korjaamiseksi ja tietoturvan ylläpitämiseksi.
Langattoman yhteyden tietoturva	Ymmärrä, miten älylukko kommunikoi langattomasti. Suosi turvallisia yhteysprotokollia.
Pilvipalvelun turvallisuus	Kiinnitä huomiota älylukon liittymiseen pilvipalveluun. Varmista, että palveluntarjoaja noudattaa tietoturvakäytäntöjä.
Fyysinen turvallisuus	Ymmärrä älylukon fyysiset turvatoimet.
Tietosuoja-asetukset	Ole tietoinen älylukon tiedonkeruusta ja jakamisesta. Tuotteiden tulisi tarjota selkeät hallintamahdollisuudet käyttäjän omasta datasta.
Valmistajan maine	Harkitse tunnettujen ja luotettavien valmistajien tuotteita.
Asiakastuki ja koulutus	Hyvä asiakastuki ja selkeä käyttöohjeistus auttavat ymmärtämään älylukon oikeanlaisen käytön ja turvallisuusnäkökohdat.
Vastuunottaminen	Ymmärrä vastuusi älylukon käytössä. Huolellinen salasanojen hallinta ja säännöllinen päivitysten tarkistus voivat vähentää riskejä.
Käytännön turvallisuusohjeet	Noudata käytännön turvallisuusohjeita, kuten avainten turvallista hallintaa ja älylukon käytön rajoituksia.
Tutustuminen ennen hankintaa	Tutustu huolellisesti älylukon tietoturvaominaisuuksiin. Lue arvosteluja ja suosituksia. Noudata valmistajan ohjeita.

Taulukko 3.2: Taulukko tietoturvaominaisuuksista

4 Yhteenveto

Älylukot ovat viime vuosina nousseet keskeiseen asemaan kodin turvallisuusratkaisuina, tarjoten käyttäjille kätevän tavan hallita ja seurata kotinsa lukitusta etänä. Tämä teknologinen murros tuo mukanaan kuitenkin myös uusia haasteita, erityisesti tietoturvan näkökulmasta. Tutkielman pääpaino on älylukkojen tietoturvassa OSI-mallin kerroksilla, mikä mahdollistaa monipuolisen tarkastelun näiden lukkojen toiminnasta ja mahdollisista riskeistä. Fyysinen kerros huomioi langattomat tai fyysiset yhteydet älylukon ja verkon välillä, siirtokerros takaa virheettömän tiedonsiirron, ja sovelluskerros tarjoaa älylukoille mahdollisuuden liittyä verkkoon ja siirtää tietoa. Päätelmänä voidaan todeta, että älykotien käyttöönotto tuo mukanaan monenlaisia tietoturvariskejä ja fyysisiä riskejä, jotka vaativat huomion kiinnittämistä kaikilla tietoturvan tasoilla. Tarkastellessa IoT-järjestelmien turvallisuutta, on huomioitava eri tietoturva-uhkien luokat, kuten matalan, keskitason ja korkean tason tietoturvauhat, jotka voivat kohdistua eri kerroksiin IoT-järjestelmissä. Näitä uhkia voivat olla esimerkiksi fyysisen kerroksen hyökkäykset, verkkokerroksen DoS-hyökkäykset, sekä sovelluskerroksen palvelukatkokset ja tietojärjestelmien luvaton käyttö.

On tärkeää tunnistaa nämä uhkat ja kehittää asianmukaisia puolustusmekanismeja estämään tai vähentämään niiden vaikutuksia. Tämä voi sisältää muun muassa vahvan salauksen käyttöä, päivitettyjen laiteohjelmistojen ylläpitämistä, käyttäjien koulutusta tietoturvahyökkäyksistä ja riskienhallintastrategioiden laatimista. Lisäksi älykotien valmistajien ja palveluntarjoajien on otettava vastuu turvallisten

tuotteiden ja palveluiden tarjoamisesta, mukaan lukien tietoturvan huomioiminen suunnittelussa ja kehityksessä.

Ensimmäisenä tutkimuskysymyksenä oli "Mitä tietoturvariskejä älylukoilla on?". Älylukkojen tietoturvariskit voidaan jakaa eri tietoturvakategorioihin, joita ovat fyysinen turvallisuus, laitteistotason riskit, verkkokerroksen uhat sekä sovelluskerroksen tietoturvauhat. Fyysisen turvallisuuden osalta älylukkojen manipulointi ja murtautuminen asuntoon ovat myös riskejä. Tämä voi mahdollistaa ulkopuolisten pääsyn kiinteistöön ilman asianmukaisia valtuuksia ja avata oven luvattomasti. Laitteistotason riskejä liittyy älylukkojen tietoturvaan ja käyttäytymiseen. Esimerkkinä näistä riskeistä ovat jamming-hyökkäykset, joissa hyökkääjä voi häiritä älylukon toimintaa ja estää pääsyn. Toisena esimerkkinä on turvattoman alustuksen riski, joka voi altistaa laitteen viestinnän väärinkäytölle. Verkkokerroksen uhkia on esimerkiksi haitallisen koodin suorittaminen verkkoyhteyden kautta, mikä voi mahdollistaa etäohjauksen ja laitteen toiminnan manipuloinnin. Toisena esimerkkina on luvaton pääsy paikallisiin verkkoresursseihin, joka voi altistaa laitteen asetusten ja verkkoviestinnän haavoittuvuudelle. Sovelluskerroksen tietoturvauhat liittyvät älylukkojen käyttämien sovellusten ja palveluiden turvallisuuteen. Näihin uhkiin kuuluvat esimerkiksi palvelukatkokset, jotka voivat vaikuttaa älylukon toimintaan ja estää pääsyn. Toisena esimerkkinä on luottamuksellisen tiedon kompromissointi ja henkilötietojen väärinkäyttö, joka voi johtaa yksityisyyden loukkauksiin ja tietomurtoihin.

Toisena tutkimuskysymyksenä oli "Millaisia käytännön suojauskeinoja voidaan soveltaa älylukkojen tietoturvan parantamiseksi?". Älylukkojen tietoturvan parantamiseksi voidaan soveltaa useita käytännön suojauskeinoja, jotka perustuvat laitteiston, ohjelmiston ja käyttäjän toimenpiteisiin. Älylukkoihin voidaan integroida murtohälytin, joka reagoi mahdollisiin murtoyrityksiin äänimerkin ja sireenihälytyksen avulla. Tämä toimii tehokkaana pelotteena tunkeutujille ja varoittaa omistajaa mahdollisista turvallisuusriskeistä. Lisäksi älylukot on suunniteltu lukittumaan

automaattisesti oven sulkeutuessa, mikä estää pääsyn ilman asianmukaisia valtuuksia. Säännölliset laiteohjelmiston päivitykset ovat tärkeitä älylukon tietoturvan ylläpitämiseksi. Päivitykset voivat sisältää korjauksia havaittuihin haavoittuvuuksiin ja parannuksia turvallisuusominaisuuksiin. Älylukko tarjoaa mahdollisuuden hallita kulunvalvontaa helposti ja turvallisesti, poistaen perinteisten avainten aiheuttamat riskit. Käyttäjä voi tarkistaa älylukon tilan ja kulkua mobiilisovelluksen avulla, mikä mahdollistaa ovensa valvonnan etänä ja käyttölokin seuraamisen. Älylukoissa käytetään AES256-salausta, joka on symmetrinen salausmenetelmä vaativa jaetun 256-bittisen avaimen viestin salaamiseen ja purkamiseen. Käyttäjät voivat omalta osaltaan varmistaa älylukkojensa turvallisuuden. Tämä sisältää mobiilisovelluspäivitysten ylläpidon, kodin internet-yhteyden suojaamisen vahvalla salasanalla sekä kaksivaiheisen tunnistautumisen käytön älylukkojen hallintasovelluksissa. Lisäksi käyttäjillä on mahdollisuus poistaa sovellus ja virtuaaliset avaimet kadonneen puhelimen tapauksessa, mikä estää luvattoman pääsyn älylukkoon.

Tutkielma syventyy Yale ja iLOQ -älylukkoihin, vertaillen niiden turvatoimintoja. Yale, osa ASSA ABLOY -konsernia, tarjoaa älylukkoja kuten Doorman L3, joka korostaa modernia muotoilua ja turvallisuusominaisuuksia. iLOQ taas erottuu omavoimaisella teknologiallaan, kuten iLOQ S5 -tuotteella, joka kerää sähkövirran NFC-puhelimesta. Älylukkojen tietoturvariskejä tarkasteltaessa keskeisiä haavoittuvuuksia nousee esiin useista näkökulmista. Yksi huomionarvoinen riski on jamming-hyökkäykset, joissa langatonta viestintää häiritään. Tämä voi mahdollistaa oven avaamisen luvattomalle pääsylle tai jopa tietojen manipuloinnille.

Älylukkojen tietoturvan parantamiseksi on tarpeen soveltaa useita käytännön suojauskeinoja, jotka kohdistuvat eri OSI-mallin kerroksiin. Säännölliset laiteohjelmiston päivitykset ovat olennaisen tärkeitä, sillä ne tuovat mukanaan turvaparannuksia vastatakseen uusiin tunnettuihin uhkiin. Älylukkoihin liittyvien mobiilisovellusten ylläpito on keskeistä, ja päivitetyt sovellukset parantavat käyttäjäkokemusta

sekä voivat sisältää tärkeitä tietoturvaparannuksia. Langattoman yhteyden ollessa usein osa älylukkojen toimintaa, vahva salasana kotiverkolle on kolmas olennainen näkökohta, varmistaen, että älylukon tiedonsiirto on suojattu langattomasti. Kaksivaiheisen tunnistautumisen käyttö älylukkoihin liittyvien mobiilisovellusten kanssa on suositeltava suojauskeino, joka merkittävästi lisää tietoturvaa. Kulunvalvontamahdollisuuksien ja käyttölokin hyödyntäminen tarjoaa toisen näkökulman, mahdollistaen omistajan seurata, kuka ja milloin ovea on avattu, tunnistaen mahdollisesti epäilyttävät toiminnot

Tutkielman taustassa esitellään molempien valmistajien historiaa ja tuotteita, korostaen niiden vahvuuksia ja sovellusalueita. Yale Doorman käyttää älykkäitä ratkaisuja koodin, kulkutunnisteen ja älypuhelimen avulla, kun taas iLOQ tuo esille paristottoman ja kestävän vaihtoehdon. Vertailu painottaa käyttäjän tarpeita ja käyttötilanteita. Sekä Yale että iLOQ ovat merkittäviä älykkäiden lukkoratkaisujen valmistajia, jotka tarjoavat monipuolisia ominaisuuksia ja vahvaa teknistä osaamista. Yale korostaa turvallisuutta ja helppokäyttöisyyttä pitkän historian ja jatkuvan innovoinnin kautta, kun taas iLOQ erottuu omavoimaisen lukitusteknologian edelläkävijänä tarjoten paristottomia ja kestäviä vaihtoehtoja perinteisille lukitusjärjestelmille. Valinta näiden kahden välillä riippuu käyttäjän tarpeista ja painotuksista, kuten käytön helppoudesta, turvallisuudesta ja integroituvuudesta laajempiin älykotijärjestelmiin. Yalen vahvuuksiin kuuluu pitkä historia ja sitoutuminen jatkuvaan innovointiin, kun taas iLOQ erottuu omavoimaisen lukitusteknologian edelläkävijänä tarjoten kestäviä ratkaisuja hajautettuihin lukostoihin.

OSI-viitemallin kautta tutkielmassa käydään läpi seitsemän kerrosta, keskittyen fyysiseen, siirto- ja verkkokerrokseen. Älylukkojen tietoturvaan liittyen esitellään yleisiä turvallisuusvaatimuksia ja tunnettuja tavoitteita kuten luottamuksellisuutta, eheyttä ja valtuutusta. Tutkielmassa mainitaan myös älykotiympäristön haasteet monimuotoisen laitekannan ja laskentatehon suhteen.

Älylukkojen tulevaisuus näyttää lupaavalta, sillä niiden kysyntä kasvaa jatkuvasti älykotien ja turvallisuusratkaisujen markkinoilla. Teknologisten innovaatioiden ja älykkään kodin trendien myötä älylukoilla on entistä suurempi rooli kodin turvallisuuden parantamisessa ja käyttömukavuuden lisäämisessä. Tulevaisuudessa älylukot mahdollisesti kehittyvät entistä monipuolisemmiksi ja integroituvat saumattomasti muihin älykotiratkaisuihin, kuten turvakameroihin, hälytysjärjestelmiin ja älykkäisiin valaistusratkaisuihin. Älylukot voisivat hyödyntää entistä enemmän tekoälyä ja koneoppimista tarjotakseen entistä älykkäämpiä ja turvallisempia ominaisuuksia, kuten käyttäjäkohtaisia tunnistusratkaisuja ja reaaliaikaista turvallisuusvalvontaa.

Yhteenvetona voidaan todeta, että tutkielma tarjoaa kattavan katsauksen älylukkojen teknisiin piirteisiin, vertailee Yalea ja iLOQ:ta sekä käsittelee tietoturvaa monipuolisesti OSI-mallin kerrosten näkökulmasta. Tutkielma luo perustan älylukkoihin liittyvälle tietoturvakontekstille ja herättää lukijan kiinnostuksen tutkimuskysymysten ja vertailun kautta. Älylukkojen suunnittelussa ja toiminnassa on huomioitu turvallisuusnäkökohdat, kuten automaattinen lukitseminen, etäohjausmahdollisuus ja kulunvalvonnan seuranta. Teknologiset ratkaisut, kuten AES256-salaus ja säännölliset laiteohjelmiston päivitykset, täydentävät kokonaisvaltaista turvallisuuskonseptia. Kuluttajille tarjotaan myös selkeää tietoa älylukkojen tietoturvaominaisuuksista, jotta he voivat tehdä perusteltuja päätöksiä tuotteiden hankinnassa.

Lähdeluettelo

[1] J. M. Batalla, A. Vasilakos ja M. Gajewski, ”Secure Smart Homes: Opportunities and Challenges”, *ACM Computing Surveys*, s. 1–32, 2017. DOI: 10.1109/ICCSN.2011.6014631.

[2] Yale. ”About us”. (2023), url: https://www.yalehome.com/fi/fi/about-us (viitattu 23. 11. 2023).

[3] A. Oy. ”Secured by ABLOY”. (2023), url: https://www.yalehome.com/fi/fi/why-yale/secured-by-abloy (viitattu 23. 11. 2023).

[4] Yale. ”Yale”. (2023), url: (https://www.yalehome.com/fi/fi) (viitattu 23. 11. 2023).

[5] Yale. ”Yale Wi-Fi Bridge”. (2023), url: https://www.yalehome.com/fi/fi/products/smart-lock-accessories/yale-connect-wi-fi-bridge (viitattu 23. 11. 2023).

[6] iLOQ. ”About us”. (2023), url: https://www.iloq.com/fi/yritys/tietoa-meista/ (viitattu 23. 11. 2023).

[7] iLOQ. ”Yleistä”. (2023), url: https://www.iloq.com/fi/ (viitattu 23. 11. 2023).

[8] W. Tanenbaum, *Computer networks*, 5. painos. Pearson, 2011, s. 63–67.

[9] Y. Li, D. Li, W. Cui ja R. Zhang, "Research based on OSI model", *2011 IEEE 3rd International Conference on Communication Software and Networks*, s. 1–4, 2011. DOI: 10.1145/3122816.

[10] M. Serror, M. Henze, S. Hack, M. Schuba ja K. Wehrle, "Towards In-Network Security for Smart Homes", *ARES '18: Proceedings of the 13th International Conference on Availability, Reliability and Security*, s. 1–8, 2018. DOI: 10.1145/3230833.3232802..

[11] M. Khawla ja M. Tomader, "A Survey on the Security of Smart Homes: Issues and Solutions", *ICSDE'18: Proceedings of the 2nd International Conference on Smart Digital Environment*, s. 81–87, 2018. DOI: 10.1145/3289100.3289114.

[12] Yale. "Privacy notice". (2023), url: (https://www.yalehome.com/global/en/privacy-and-legal-center/privacy-notice) (viitattu 24. 11. 2023).

[13] Yale. "Älylukko tuo turvaa". (2023), url: (https://www.yalehome.com/fi/fi/innostu-alytuotteista/blogi/alylukot/alylukko-tuo-turvaa) (viitattu 24. 11. 2023).

[14] A. Zhang ja R. V. Kandubai, "Access Control Schema for Smart Locks using a Wifi Bridge: An exploration of a smart lock access control system based around the SimSim retrofitting smart lock.", *ICRAI '20: Proceedings of the 6th International Conference on Robotics and Artificial Intelligence*, s. 174–178, 2021. DOI: 10.1145/3449301.3449331.