Älykaiuttimien tietoturva ja yksityisyys

Turun yliopisto
Tietotekniikan laitos
TkK-tutkielma
Tieto- ja viestintätekniikka
Helmikuu 2024
Tomas Alivuotila

TURUN YLIOPISTO
Tietotekniikan laitos

Tomas Alivuotila: Älykaiuttimien tietoturva ja yksityisyys

TkK-tutkielma, 22 s.
Tieto- ja viestintätekniikka
Helmikuu 2024

Älykaiuttimet ovat verkkoon yhdistettyjä ja puheentunnistuksen omaavia kaiuttimia, joiden avulla käyttäjä voi suorittaa erilaisia toimintoja puheen avulla. Yhteys internetiin ja puheentunnistus tuovat myös mukanaan tietoturvallisia ja yksityisyyteen liittyviä huolia. Tutkielman tavoitteena on perehtyä tietoturvariskeihin ja yksityisyyshuoliin. Lisäksi perehdytään Amazonin, Googlen ja Applen älykaiuttimien tietoturvaa ja yksityisyyttä käsitteleviin verkkosivuihin
Tietoturvariskien tutkimista tuetaan älykaiuttimen ekosysteemillä ja viitemallilla. Tutkielmassa käytetään OSI-viitemallia, joka koostuu seitsemästä kerroksesta. Mahdolliset kyberhyökkäykset kohdistuvat viitemallin eri kerroksiin. Lisäksi älykaiuttimen ekosysteemin eri osat luovat tietoturvauhkia. Puheentunnistus ja datankeruu herättävät yksityisyyshuolia. Äänidatan keruu on välttämätöntä, jotta älykaiuttimelle annetut komennot voivat toteutua.
Älykaiuttimiin liittyviä tietoturvariskejä ja yksityisyyshuolia on monia. Kuluttajalle yksityisyyshuolet ovat keskeisimpiä. Oleellista on ymmärtää käytettävyyden ja yksityisyyden tasapainottaminen. Valmistajien verkkosivuilta löytyy runsaasti informaatiota älykaiuttimien tietoturvasta. Jokaisella valmistajalla oli samankaltaisia lähestymistapoja. Verkkosivut voisivat kuitenkin olla lukijaystävällisemmät ja helpommin lähestyttävät.

Asiasanat: Älykaiutin, Puheentunnistus, Äänidata, Esineiden internet

Sisällys

1 Johdanto

Älykaiuttimen avulla käyttäjän on mahdollista tehostaa jokapäiväistä elämäänsä ja lisätä arjen mukavuutta. Näiden kaiuttimien myyntivaltti on puheentunnistus. Käyttäjä voi milloin vain esimerkiksi kysyä kaiuttimelta päivän säätiedotuksen, pyytää soittamaan musiikkia tai asettamaan herätyksen seuraavalle päivälle. Jatkuvasti kuunteleva kaiutin voi vastata kysymykseen tai toteuttaa käskyn välittömästi. Älykaiuttimien puheentunnistus sisältää myös turvallisuusriskejä. Erään tutkimuksen mukaan älykaiuttimien omistajilla on merkittäviä huolia omaa yksityisyyttään kohtaan [1].

Tämä tutkielma keskittyy älykaiuttimien tietoturvaan ja yksityisyyteen. Tutkimuksen tarkoituksena on syvällisesti analysoida älykaiuttimien haavoittuvuuksia sekä käyttäjän mahdollisuuksia vaikuttaa niiden tietoturvaan ja samalla arvioida sitä, kuinka merkittäviä vaikutusmahdollisuudet ovat. Koska älykaiuttimet toimivat esineiden internetin (Internet of Things, IoT) keskiönä [2], muodostavat ne mielenkiintoisen tutkimuskohteen. Tarkoituksena on selvittää, onko älykaiutin varteenotettava tietoturvallisuusriski. Lisäksi tutkitaan suurien laitevalmistajien tietoturva- ja yksityisyyskäytäntöjä. Tutkielmalla on kaksi tutkimuskysymystä:

Tk1a: Mitä tietoturva- ja yksityisyyshuolia älykaiuttimiin liittyy?

Tk1b: Ovatko mahdolliset tietoturva- ja yksityisyyshuolet merkittäviä kuluttajanäkökulmasta?

Tk2: Mitä johtavat laitevalmistajat sanovat älykaiuttimien tietoturvasta ja yksityisyydestä?

Tutkielman lähteet ovat pääosin informaatioteknologian tietokannoista, erityisesti Association for Computing Machinery (ACM) ja Institute of Electrical and Electronics Engineers (IEEE) -tietokannoista. Tiedonhaku suoritettiin englanniksi, ja keskeiset hakusanat olivat: smart speaker, alexa, security, privacy, cyberattack ja voice assistant. Lähes kaikki lähteet ovat yliopistoissa suoritettuja tutkimuksia. Lisäksi hyödynnettin eri laitevalmistajien verkkosivuja tietoturva- ja yksityisyyspolitiikan tutkimisessa. Lähteiden valinnassa suurin rajaaja oli julkaisuvuosi. Älykaiuttimien nopean kehityksen kannalta vanhat tutkimukset voivat olla harhaanjohtavia tai vanhentuneita. Kokonaisuudessaan lähteidenhakuprosessi oli kaksivaiheinen. Aluksi haettiin lähteitä tietokannoista hakusanoja käyttäen. Tämän jälkeen pyrittiin hyödyntämään valittujen julkaisujen lähdeluetteloa lähteiden haussa.

Tutkielmassa on kolme asialukua. Luvussa 2 perehdytetään lukija älykaiuttimen ekosysteemiin ja viitemalliin. Luvussa 3 perehdytään älykaiuttimen tietoturvaan ja yksityisyyteen sekä analysoidaan tuloksia. Luvussa 4 perehdytään suurimpien laitevalmistajien tietoturva- ja yksityisyyskäytäntöihin. Luku 5 on yhteenveto, jossa myös vastataan tutkielman tutkimuskysymyksiin.

2 Älykaiuttimen ekosysteemi ja viitemalli

Jotta voidaan syventyä älykaiuttimien yksityisyyteen ja tietoturvaan, on tärkeä hahmottaa älykaiuttimen ekosysteemi. Älykaiuttimen ekosysteemillä tarkoitetaan esimerkiksi kodin IoT-ympäristöä. Kun hahmotetaan erilaisten toimintojen kulku ekosysteemissä, on huomattavasti helpompi ymmärtää, millaisia riskejä saattaa ilmetä käyttäjän käyttäessä älykaiutinta. Tässä tutkielmassa viitemalli älykaiuttimen ekosysteemistä toimii laitteen yksityisyyteen ja tietoturvaan liittyvien kysymysten perustana. Tämä malli auttaa hahmottamaan älykaiuttimen roolin kodin IoT-ympäristössä ja sen vuorovaikutusta eri osien kanssa. Se tarjoaa puitteet ymmärtää riskejä ja mahdollisia uhkia, joita käyttäjä saattaa kohdata älykaiutinta käyttäessä. Seuraavaksi tarkastellaan älykaiuttimen ekosysteemiä ja hahmotellaan sen viitemalli.

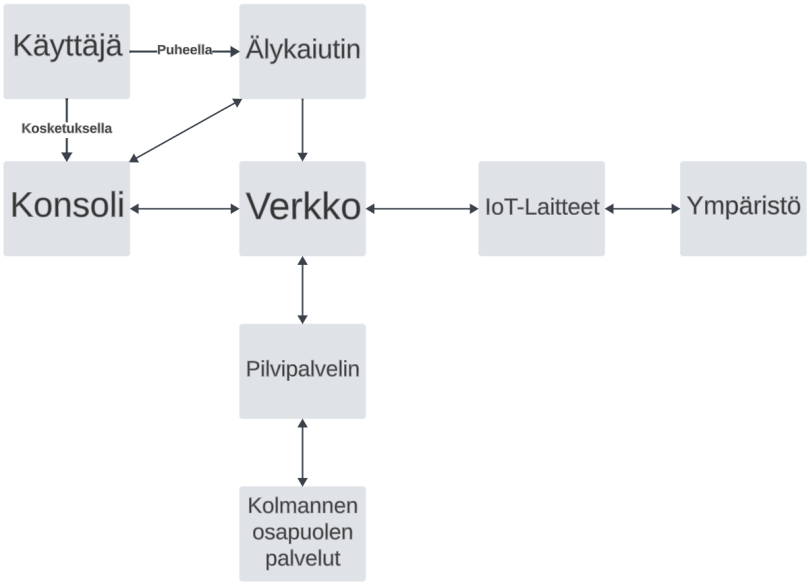
2.1 Ekosysteemi

Kuvasta 2.1 ilmenee, että kokonaisuudessaan älykaiuttimen ekosysteemi koostuu seitsemästä eri osasta: älykaiuttimesta, konsolista, verkosta, IoT-laitteista, ympäristöstä, pilvipalvelimesta ja kolmannen osapuolen palveluista. Ympäristöä lukuun ottamatta älykaiuttimen ekosysteemin osat ovat yhteydessä toisiinsa verkkoviestinnän kautta. Yleisimmät viestinnän tekniikat ovat WiFi, Bluetooth ja ZigBee. [3]

Käyttäjällä on yhteys ekosysteemiin älykaiuttimen ja konsolin kautta. Älykaiuttimen avulla käyttäjä voi kommunikoida suullisesti virtuaaliavustajan kanssa, jonka avulla hän voi lähettää käskyjä tai pyyntöjä pääosin koskien muita Iot-laitteita tai kolmannen osapuolen palveluita. Konsolilla tarkoitetaan valmistajan tarjoamaa sovellusta, jonka avulla voi hallita IoT-ympäristöä. Sovelluksen avulla käyttäjä voi esimerkiksi parittaa IoT-laitteita älykaiuttimeen, hallita kaiuttimen asetuksia ja kommunikoida virtuaaliavustajan kanssa. [3]

Älykaiuttimen ekosysteemissä IoT-laitteilla tarkoitetaan muita älylaitteita, jotka ovat osa älykodin IoT-ympäristöä.Ympäristöllä tarkoitetaan esimerkiksi käyttäjän kotia, jonka valaistus, ilmankosteus tai lämpötilä voi vaihdella IoT-laitteiden vaikutuksesta. Ympäristön muutos voi myös käynnistää IoT-laitteen. Esimerkiksi älyilmastointilaite voi käynnistyä lämpötilan noustessa määritettyä maksimiarvoa korkeammaksi. [3]

Pilvipalvelimessa tapahtuu äänidatan prosessointi sekä tekstidatan välittäminen kolmansille osapuolille ja IoT-laitteille. Kolmannen osapuolen palveluilla tarkoitetaan esimerkiksi musiikkipalveluita ja sosiaalisia medioita. [3]



Kuva 2.1: Älykaiuttimen ekosysteemi(perustuu artikkelin [3] kuvaan)

2.2 Viitemalli

Älykaiuttimen ekosysteemiä voidaan mallintaa OSI-viitemallilla (engl. Open Systems Interconnection Reference Model, OSI reference model). OSI-malli luotiin 1970-luvun lopulla kansainvälisen standartoimisjärjestö ISO:n (International Organization for Standardization) toimesta, jotta tietokoneet voisivat kommunikoida myös muidenkin valmistajien tietokoneiden kanssa. OSI-malli kuvaa verkkoarkkitehtuuria. Se mahdollistaa datan siirtämisen tietokonejärjestelmien välillä seitsemässä kerroksessa. OSI-malli jakaantuu seitsemään kerrokseen, joka rakentuu alhaalta ylöspäin seuraavassa järjestyksessä: fyysinen kerros (engl. physical layer), siirtokerros (data link layer), verkkokerros (network layer), kuljetuskerros (transport layer), istuntokerros (session layer), esitystapakerros (presentation layer) ja sovelluskerros (application layer). Alhaisempi kerros suorittaa aina alkeellisempia tehtäviä kuin sitä ylempi kerros. Älykaiuttimelle oleelliset kerrokset ovat fyysinen kerros, siirtokerros, verkkokerros, kuljetuskerros ja verkkokerros.[4]

Fyysisen kerros määrittelee ekosysteemin fyysiset osat. Sen tehtävänä on kerätä

dataa. Esimerkiksi älykaiuttimen mikrofoni on osa fyysistä kerrosta. Kuljetuskerros koostuu kahdesta alakerroksesta: Media Access Control (MAC) ja Logical Link Control (LLC). MAC-kerros määritteleee laitteisto-osoitteet (MAC-osoitteet), jotka ovat älykaiuttimen ekosysteemin laitteiden fyysiset osoitteet. MAC-osotteiden avulla tietoliikenne ohjataan oikeisiin kohteisiin. LLC-kerros huolehtii linkin hallinnasta verkkokerroksen ja MAC-kerroksen välillä. Tämä kerros huolehtii myös virheiden korjauksesta ja virheiden havaitsemisesta. LLC-kerros varmistaa, että siirretty data on oikeassa järjestyksessä ja tarvittaessa suorittaa korjauksia mahdollisiin virheisiin. Lisäksi LLC takaa tehokkaan yhteyden hallinnan ja kommunikoinnin näiden kahden alakerroksen välillä, mikä on olennaista luotettavan tietoliikenteen varmistamiseksi verkossa.[5][4]

Verkkokerros mahdollistaa tietokonejärjestelmien välisen tiedonsiirron verkossa. Se käsittelee kohdejärjestelmien ja -palvelimien tunnistamista, osoitteiden hallintaa ja tiedon reitittämistä. Verkkokerros auttaa älykaiutinta tunnistamaan pilvipalvelimen IP-osoitteen. Se myös varmistaa, että äänidata reititetään älykaiuttimesta pilvipalvelimeen sekä tarvittaessa pilvipalvelimen ja muiden IoT-laitteiden välillä. Esimerkiksi, jos käyttäjä pyytää äänikomennolla älykaiutinta sytyttämään älyvalot, verkkokerros voi osallistua tiedonsiirron hallintaan varmistaen, että äänikomento reititetään oikeaan suuntaan ja saavuttaa älyvalot pilvipalvelimen kautta.[4]

Kuljetuskerros mahdollistaa älykaiuttimen ja muiden laitteiden välisen yhteyden muodostamisen ja varmistaa luotettavan tiedonsiirron. Kuljetuskerros hallinnoi tiedonvirtaa älykaiuttimen ja muiden IoT-laitteiden välillä. Samalla se huolehtii pakettien jakamisesta pienempiin osiin, tarkistaa mahdolliset virheet ja tunnistaa tarvittavat palvelut. Älykaiuttimen ekosysteemissä sovelluskerros mahdollistaa älykaiuttimen ja muiden laitteiden sovellusten yhteyden verkkoon. Se tarjoaa rajapinnan, joka sallii erilaisten sovellusten käyttää älykaiuttimen verkko-ominaisuuksia.[4]

3 Älykaiuttimen tietoturva ja yksityisyys

Älykaiutin on Internetiin yhdistetty kaiutin, joka on jatkuvasti valmiustilassa. Se aktivoituu kuultuaan tietyn avainsanan, joka vaihtelee eri laitevalmistajien mukaan (esimerkiksi "Alexa", "Hey Siri"tai "Hey Google"). Kun käyttäjä on maininnut avainsanan, voi hän alkaa esittämään pyyntöjä tai käskyjä älykaiuttimelle. Tämä äänidata käsitellään laitevalmistajan ääniohjausteknologian avulla (engl. voice assistant technology) [6]. Äänidataa ei kuitenkaan käsitellä paikallisesti itse laitteessa, koska automaattinen puheentunnistus (automatic speech recognition, ASR), luonnollisen kielen ymmärtäminen ja tuottaminen (natural language understanding and generation, (NLU, NLG)) sekä käyttäjän pyyntöihin tai käskyihin vastaaminen on teknisesti varsin vaativaa [7]. Älykaiuttimet vaativat ympärilleen tietynlaisen ekosysteemin, joka mahdollistaa älykaiuttimien toiminnan IoT-ympäristöissä.

Älykaiuttimen tärkein osa on sen virtuaaliavustaja (voice assistant). Virtuaaliavustajat ovat tekoälyyn perustuvia ohjelmia, jotka luovat suullisen käyttöliittymän käyttäjän ja laitteen välille. Jokaisella suurella laitevalmistajalla on oma virtuaaliavustajansa. Tutkielman kannalta oleellisimmat ovat Google Assistant (Google, 2016), Alexa (Amazon, 2014) ja Siri (Apple, 2010). Virtuaaliavustajat eivät ole yksinomaan älykaiuttimien ominaisuus, vaan esimerkiksi nykypäivän älypuhelimet sisältävät myös virtuaaliavustajan. Eri virtuaaliavustajilla voi olla uniikkeja toiminnal-

lisuuksia, mutta pääasiassa jokainen avustaja toimii samalla periaatteella. Se mikä tekee virtuaaliavustajista vaikuttavia, on niiden monipuolinen ja laaja toimintovalikoima. Sen mahdollistaa jatkuva yhteys Internetiin. [8]

3.1 Älykaiuttimen tietoturva

Tässä alaluvussa kartoitetaan älykaiuttimeen ja sen ekosysteemiin liittyviä tietoturvariskejä ja esitellään mahdollisia kyberhyökkäyksiä, joita älykaiuttimeen voi kohdistua. Mitä enemmän ekosysteemissä on kolmannen osapuolen palveluita ja IoT-laitteita, sitä todennäköisempiä kyberhyökkäykset ovat. Perehdytään mahdollisiin älykaiuttimen tietoturvallisiin haavoittuvuuksiin käyttäen apuna edellisessä alaluvussa esitettyä älykaiuttimen ekosysteemiä ja viitemallia.

Fyysisen kerroksen hyökkäykset kohdistuvat suoraan älykaiuttimeen sisäisten- ja ulkoisten porttien tai sensorien kautta. Esimerkiksi USB-portin kautta voidaan pyrkiä esimerkiksi saamaan pääsy älykaiuttimen ydinkäyttäjän tasolle (engl. root shell)[2]. Lisäksi älykaiuttimien puheentunnistusjärjestelmät ovat alttiita äänipohjaisille hyökkäyksille. Etä-äänihyökkäykset ovat tapa antaa käskyjä älykaiuttimelle etäältä. Eräs esimerkki tällaisesta hyökkäyksestä on delfiinihyökkäys, joka käyttää ultraääntä. Tämä hyökkäystapa lähettää ultraäänellä kaksi äänikomentoa, joista ensimmäinen on suunniteltu aktivoimaan älykaiutin avainsanalla ja toinen sisältää käskyn tai pyynnön älykaiuttimelle. Kyseinen hyökkäys voi olla hankala havaita, sillä ihmiskorva ei havaitse ultraääntä. [9][10]

Siirtokerroksen tasolla älykaiuttimet ovat esimerkiksi haavoittuvaisia välttämättömän WiFi-yhteyden vuoksi. Jamming-hyökkäykset ovat palvelunestohyökkäyksiä (engl. denial of service attack, dos attack). Ne voivat kohdistua langattomaan radioliikenteeseen, kuten Wi-Fiin, häiritsemällä signaaleja ja aiheuttamalla häiriötä, mikä voi vaikuttaa merkittävästi langattoman viestinnän luotettavuuteen. Jamming-hyökkäys onnistuu häiritsemään WiFi-yhteyttä peittämällä oikeat signaalit huomat-

tavasti suuritehoisemmalla meluisammalla signaalilla. Tämä laskee Signaali-kohinasuhdetta (engl. signal-to-noise ratio, SNR), mikä voi pahimmassa tapauksessa johtaa yhteyden menettämiseen. Jamming-hyökkäykset ovat varteenotettava uhka, koska niiden toteuttaminen on helppoa ja edullista.[11]

Väliintulohyökkäykset (engl. man in the middle attack, MITM attack) ovat myös uhka älykaiuttimen ekosysteemille. Nämä hyökkäykset tapahtuvat viitemallin verkkokerroksessa, kuljetuskerroksessa ja istuntokerroksessa. MITM-hyökkäys on tilanne, jossa hyökkääjä asettuu salaa kahden osapuolen välisen viestinnän väliin. Tämän avulla hyökkääjä voi salakuunnella ja mahdollisesti myös muokata lähetettyä informaatiota. Älykaiuttimen ekosysteemissä hyökkääjä voi salakuunnella verkkovirtaa ja lisätä tai muokata käskyjä. Ekosysteemistä voi löytyä heikkouksia, joiden avulla hyökkääjä voi esimerkiksi varastaa käyttäjätietoja ja muokata älykaiuttimen asetuksia.[2][12]

Sovelluskerroksen haavoittuvuudet perustuvat muun muassa älykaiuttimen ekosysteemin käyttämiin sovelluksiin. Monet IoT-laitteet vaativat käyttäjää lataamaan valmistajan sovelluksen, jonka avulla IoT-laite voidaan kytkeä verkkoon ja yhdistää muihin laitteisiin. Hyökkääjä voi hyväksikäyttää sovellusten mahdollisia haavoittuvuuksia, jotka ovat jääneet valmistajilta huomaamatta. Siksi on tärkeää varmistaa, että käytössä on aina uusin versio sovelluksista. Hyökkääjä voi myös väärinkäyttää palvelinsovelluksia, kuten ASR ja NLU. Kuten aiemmin tässä luvussa mainittiin, nämä palvelinsovellukset vastaavat äänidatan prosessoinnista. [2]

3.1.1 Hyökkäysten ehkäisykeinoja

Älykaiuttimien tietoturvan parantaminen on vaikea aihe. Parantaessa kaiuttimen tietoturvaa on otettava huomioon myös sen käytettävyys. On tärkeää ylläpitää laitteen käyttäjäystävällisyyttä samalla, kun suojaudutaan mahdollisilta uhilta. Seuraavat esitetyt ehkäisykeinot ottavat huomioon myös älykaiuttimen käyttäjäystäväl-

lisyyden säilymisen.

Fyysisen kerroksen hyökkäyksiä vastaan voisi puolustautua esimerkiksi minimoimalla älykaiuttimen porttien määrän. Ulkoiset portit, kuten USB-portit, voisi mahdollisesti peittää, jolloin niihin käsiksi pääsy olisi edes hieman hankalampaa. Etääänihyökkäyksiltä on mahdollista suojautua opettamaan virtuaaliavustaja erottamaan kaiuttimesta tuleva ääni ja ihmisen ääni[13]. Jamming-hyökkäykseltä voi suojautua esimerkiksi tarkkailemalla signaalien voimakkuuksia [14].

On myös tärkeää ottaa huomioon käyttäjän asema älykaiuttimen tietoturvassa. Kyberhyökkäyksen riski pienenee huomattavasti, kun käyttäjällä on edes vähän ymmärrystä laitteesta ja turvallisesta internet-käyttäytymisestä. Esimerkiksi vahvat salasanat tekevät älykaiuttimien ja muiden IoT-laitteiden käytöstä turvallisempaa. Pitkän ja monimutkaisen salasanan käyttö nostaa salasanan turvatasoa merkittävästi [15]. Lisäksi mahdollisten riskien tiedostaminen auttaa käyttäjää ennaltaehkäisemään hyökkäyksiä ja toimimaan oikein tilanteissa, joissa hän on joutunut hyökkäyksen kohteeksi.

3.2 Käyttäjän yksityisyys

Suurimmalla osalla älykaiuttimien käyttäjistä on rajoitetusti tietoa siitä, miten älykaiuttimet käytännössä toimivat [6], [16]–[22]. Epätietoisuus älykaiuttimien toiminnallisuuksista voi vaikuttaa käyttäjän asenteeseen älykaiuttimia kohtaan ja määrittää sen, mihin tarkoituksiin kaiutinta ylipäätään käytetään. Ymmärtämällä paremmin, miten älykaiuttimet keräävät ja käsittelevät tietoa, käyttäjät voivat tehdä tietoisempia päätöksiä siitä, mitä tietoja he haluavat jakaa ja mitä eivät. Älykaiuttimien kasvava suosio [23] tekee yksityisongelmien ymmärtämisestä entistä tärkeämpää. Erityisesti kolme seikkaa nousee esiin pohdittaessa älykaiuttimiin liittyviä yksityisyysongelmia.

Ensimmäinen huomionarvoinen seikka on älykaiuttimien puheentunnistus. Ku-

ten jo aiemmin mainittiin, laitevalmistajat keräävät äänidataa parantaakseen virtuaaliavustajien toimivuutta. Laitevalmistajat sanovat, että äänidataa kerätään vasta älykaiuttimen kuultua avainsanan[1] [2]. Avainsanan väärintulkinta on kuitenkin oleellinen huoli [24]. Älykaiutin voi siis ruveta keräämään äänidataa tulkittuaan väärin sanan, joka enemmän tai vähemmän muistutti laitteen avainsanaa. Kerätty äänidata voi esimerkiksi olla arkaluontoista, jolloin käyttäjä ei halua älykaiuttimen keräävän sitä.

Toinen seikka on älykaiuttimien sijainti. Kuluttajanäkökulmasta tarkastaltaessa älykaiuttimet sijaitsevat lähes poikkeuksetta käyttäjän kotona. Käyttäjän koti on yksi älykaiuttimiin liittyvistä yksityisyydensuojaa eniten koskettavista paikoista tietojen keräämisen näkökulmasta [6]. Olisi esimerkiksi mahdollista määrittää älykaiuttimen omistavan perheen arkirytmi ja perheenjäsenten lukumäärä ainoastaan äänidatan avulla tarkkailemalla älykaiuttimen keräämän datan kellonaikoja ja erottuvien uniikkien äänien lukumäärää.

Kolmas seikka on älykaiuttimen käytössä olevat kolmannen osapuolen sovellukset. Älykaiuttimen avulla käyttäjä voi hallita monia kolmannen osapuolen sovelluksia. Näiden sovellusten käyttö älykaiuttimien alustoilla saattaa tuoda esiin vakavampia yksityisyyteen liittyviä riskejä verrattuna pelkästään alustan omien sovellusten käyttöön, koska sovellusmarkkinat ovat suhteellisen avoimet [25]. Muun muassa älyvalaisimet vaativat sovelluksen, jonka avulla niitä voidaan kontrolloida esimerkiksi puhelimen tai älykaiuttimen avulla. Kun käyttäjä pyytää älykaiutinta sytyttämään kodin älyvalot, data kulkeutuu aluksi laitevalmistajan pilvipalvelimelle, josta se kulkeutuu tekstinä älyvalaisimen pilvipalvelimelle. Tämän jälkeen pyyntö toteutetaan ja valot syttyvät.

[1] https://policies.google.com/privacy?hl=en

[2] https://www.amazon.com/gp/help/customer/display.html?nodeId=GX7NJQ4ZB8MHFRNJ

3.3 Pohdintaa

Kuluttajanäkökulmasta älykaiuttimet ovat varsin tietoturvallisia. On realistista luottaa siihen, että esimerkiksi Google ja Amazon tuovat markkinoille vain tietoturvallisia laitteita. Älykaiuttimen merkittävät ominaisuudet ovat puheentunnistus ja virtuaaliavustaja. Kuluttajatasolla jatkuvasti kuunteleva kaiutin ei luo merkittäviä tietoturvariskejä. Aikaisemmin mainittujen kyberhyökkäysten tapahtuminen käytäjälle on erittäin epätodennäköistä. On tärkeää kuitenkin ymmärtää, että mikään laite ei ole täysin tietoturvallinen. Todennäköisimmin käyttäjä joutuu kyberhyökkäyksen kohteeksi heikkojen salasanojen vuoksi. Tältä voi suojautua esimerkiksi salasanan hallintasovellusten ja kaksivaiheisen tunnistautumisen avulla.

Älykaiuttimet luovat runsaasti yksityisyyshuolia. Kun kuluttaja ostaa älykaiuttimen, on hänen hyväksyttävä se, että hänen dataansa tullaan käyttämään toimivuuden parantamiseen ja mahdollisesti myös mainontaan. Älykaiuttimien kannalta käytännöllisyys ja yksityisyys luovat lähes mahdottoman yhtälön. Jos älykaiuttimien yksityisyyttä parannetaan huomattavasti, niiden käytännöllisyys tulee kärsimään jossain määrin. Käyttäjien tulisi olla tietoisia omista mahdollisuuksistaan vaikuttaa älykaiuttimen yksityisyysasetuksiin. Tämä edellyttää käyttäjiltä aktiivista tietoisuutta siitä, miten heidän henkilötietojaan käytetään ja säilytetään. Samalla yritysten on oltava täysin läpinäkyviä siitä, miten ne käsittelevät käyttäjien tietoja ja mitä toimenpiteitä ne toteuttavat yksityisyyden suojaamiseksi.

Kokonaisudessaan yksityisyyshuolet ovat käyttäjälle merkittävämpiä kuin tietoturvariskit. Harkitessaan älykaiuttimen ostamista, käyttäjän tulee ymmärtää laitteeseen liittyvät yksityisyyshuolet ja puheentunnistuksen toiminnallisuudet. Laitteen käyttötarkoituksella on kuitenkin suuri rooli yksityisyyden kannalta. Mitä enemmän sovelluksia ja laitteita on yhdistettynä älykaiuttimeen, sitä enemmän käyttäjän dataa käytetään.

4 Johtavien laitevalmistajien tietoturvaseloste ja yksityisyydensuoja

Tässä luvussa syvennytään johtavien laitevalmistajien yksityisyydensuojaan ja tietoturvakäytäntöihin. Käydään läpi, miten kyseiset valmistajat huolehtivat käyttäjiensä yksityisyydestä ja tarjoavat turvallisen digitaalisen ympäristön. Pohditaan myös, mitä toimenpiteitä he ovat tehneet varmistaakseen laitteidensa ja palveluidensa tietoturvan. Lisäksi tarkoituksena on arvioida näiden laitevalmistajien verkkosivuja. Huomio kiinnittyy erityisesti informaation määrään ja saatavuuteen. Lähteinä käytetään pääosin vain valmistajien omia sivuja. Johtavat älykaiuttimen laitevalmistajat ovat Amazon, Google ja Apple, joista suosituin on Amazon[23].

4.1 Amazon Echo

Amazon Echo ilmestyi markkinoille vuonna 2014 [6], [26]. Myöhemmin Amazon on julkaissut lukuisia muita malleja tarjotakseen käyttäjille lisää vaihtoehtoja heidän ostaessaan älykaiutinta Amazonilta.[1]. Echo-laitteilla on joitain eroavaisuuksia, mutta niiden toimintaperiaate on sama. Amazon Echo -laitteita hallinnoidaan Amazon Alexa- sovelluksella, jonka käyttämiseen käyttäjä tarvitsee Amazon-tilin.

[1]https://www.amazon.com/gp/help/customer/display.html?nodeId=GHRYQ6GHE4A5TUD2

Amazonin verkkosivuilla on sivu, joka pyrkii vastaamaan käyttäjien yleisimpiin yksityisyyskysymyksiin. Sivustolla kerrotaan esimerkiksi Echo-laitteen kuuntelemisesta ja tiedonkeruusta. Sivustolla on myös linkki, joka ohjaa sivustolle, jossa kerrotaan tarkemmin Alexan tietoturvasta ja yksityisyydestä[2].[27]

Amazon kertoo Echo-laitteiden kuuntelevan vasta kuultuaan avainsanan tai käyttäjän aktivoidessa Alexan painamalla älykaiuttimessa olevaa painiketta. Joillakin laitteilla käyttäjä voi halutessaan myös aktivoida seurantatilan, jonka avulla käyttäjä voi esittää monta pyyntöä älykaiuttimille ilman, että hänen tarvitsee toistaa avainsanaa jokaisen pyynnön välissä. Osa Echo-laitteista voi myös aktivoitua esimerkiksi lasin rikkoutumisen tai palohälyttimen äänestä. Vakiona Echo-laitteet kuitenkin aktivoituvat ainoastaan avainsanan tai painalluksen avulla. Käyttäjä tietää Echo-laitteen kuuntelevan häntä, kun laitteen merkkivalo palaa tai vaihtaa väriä. Echo-laitteissa on myös mikrofonin mykistyspainike. Kun mikrofoni on mykistettynä, punainen merkkivalo syttyy ja laite ei voi kuunnella käyttäjää.[27]

Käyttäjien äänidataa käytetään esimerkiksi Alexan puheentunnistuksen ja luonnollisen kielen ymmärtämisen parantamiseen. Amazonin mukaan käyttäjien äänidata on pakollista, jotta Alexan toimivuutta voidaan parantaa. Amazon kuitenkin antaa käyttäjille mahdollisuuden tarkkailla ja hallita heidän äänidataansa. Lisäksi käyttäjillä on mahdollisuus poistattaa äänidata automaattisesti tietyn aikarajan jälkeen. Käyttäjä voi myös kieltää Amazonia tallentamasta äänidataa. Tässä tapauksessa koko äänidatahistoria poistetaan ja tulevaisuudessa äänidata poistetaan heti prosessoinnin jälkeen. Amazon kuitenkin huomauttaa, että äänidatan poistaminen voi heikentää käyttäjäkokemusta. Jotkin Echo-laitteet myös tukevat paikallista äänidatan käsittelyä. Tässä tapauksessa äänidataa ei prosessoida pilvessä, vaan se hoidetaan älykaiuttimen sisällä.[27]

Amazon varmistaa Echo-laitteiden tietoturvan kuuden eri turvallisuuskerroksen

[2]amazon.com/alexaprivacy

avulla: ohjelmiston aitoustarkistus, sovelluksen turvallisuustarkistukset, automaattinen turvallisuusskannaus, haavoittuvuuden havaitsemistestaus, tuki turvallisuusyhteisöltä, automaattiset turvallisuuspäivitykset.[28]

Ohjelmiston aitoustarkistus -kerroksen tavoitteena on varmistaa ohjelmiston toimivuus ja autenttisuus. Lisäksi Echo-laitteet varmistavat uusien ohjelmistojen olevan kunnossa ennen jokaista ohjelmistopäivitystä. Echo-laitteissa on ollut vuodesta 2017 alkaen turvallinen käynnistys (engl. secure boot). Sen tarkoituksena on vahvistaa laitteiston autenttisuus jokaisen käynnistyksen yhteydessä. Sovelluksen turvallisuustarkistukset -kerroksessa uuden älykaiuttimen uudet ominaisuudet arvioidaan. Lisäksi suoritetaan uhkanmallinnusta, koodin arviointia ja turvallisuustestauksia.[28]

Automaattinen turvallisuusskannaus -kerroksen tehtävänä on automaattisesti skannata ohjelmistoa haavoittuvuksien varalta. Skannaamiseen käytetään talon omia työkaluja sekä kolmannen osapuolen työkaluja. Skannaus on käynnissä jatkuvasti, joten mahdollisiin haavoittuvuuksiin voidaan reagoida mahdollisimman nopeasti. Haavoittuvuuden havaitsemistestaus -kerroksessa suoritetaan jatkuvaa turvallisuustestausta Echo-laitteissa ja Alexan palveluissa. Testauksiin on palkattu turvallisuusalan osaajia. Lisäksi Amazon tekee yhteistyötä turvallisuusläpäisytestausta suorittavien yritysten kanssa.[28]

Amazon on myös hakenut tukea turvallisuusyhteisöltä. Amazon Vulnerability Research Program (VRP) on ohjelma, joka tarjoaa rahaa löydettyjä turvallisuusongelmia vastaan. VRP:n avulla Amazon löytää haavoittuvuuksia muiden ihmisten avulla. Amazon on myös luvannut tarjota ohjelmiston turvallisuuspäivityksiä ainakin siihen saakka, kunnes kyseistä laitetta ei ole luokiteltu uudeksi laitteeksi Amazonin verkkosivuilla neljään vuoteen. Amazon kuitenkin pyrkii päivittämään laiteita mahdollisimman pitkään.[28]

4.2 Google Nest

Google julkaisi Google Home -kaiuttimen vuonna 2016 [29]. Vuonna 2018 Google ja Nest yhdistyivät muodostaen brändin Google Nest [30]. Googlella on huomattavasti vähemmän erilaisia älykaiuttimia[3] kuin Amazonilla. Kaiuttimet ovat toimintaperiaatteeltaan samanlaisia lukuun ottamatta Google Nest Hub:ia ja Google Nest Hub Max:ia, joissa on lisäosana kosketusnäyttö. Google Nest -laitteita hallinnoidaan Google Home -sovelluksella, jonka käyttäminen vaatii Google-tiliä.

Googlen sivuilta löytyy kattavasti tietoa laitteiden tietoturvasta ja yksityisyydestä. He esittävät lukuisia sitoumuksia, kuten esimerkiksi teknisten tietojen avoimuus, julkaistu tunnistinopas, vastuulliset mainostuskäytännöt ja itsenäinen turvallisuustodennus[4]. Googlen sivuilta voi myös löytää sivun, jossa vastataan yleisimpiin yksityisyys- ja tietoturvakysymyksiin[5]. Perehdytään seuraavaksi Googlen yksityisyys- ja tietoturvakäytäntöihin koskien Nest-laitteita.[31]

Kuten Echo-laitteet, myös Nest-laitteet tallentavat äänidataa vasta avainsanan kuultuaan. Myös Nest-laitteissa palaa merkkivalo, kun kaiutin kuuntelee käyttäjää ja lähettää äänidataa Googlelle. Google ei oletuksena tallenna äänitallenteita, vaan käsittelee tallenteen ja tallentaa sen tekstinä. Nest-laitteiden mikrofoni on myös mykistettävissä. Tallennettu äänidata tallennetaan Googlen palvelimille. Jotkin laitteet kuitenkin tallentavat ja käsittelevät osan äänidatasta paikallisesti. Tallennettu äänidata on poistettavissa Googlen sivujen kautta. Google myös kertoo, että äänidataa ei käytetä mainosten personointiin. Google voi kuitenkin päätellä käyttäjän ja Nest-laitteen välisten keskustelujen perusteella käyttäjän mielenkiinnon kohteita. Käyttäjä voi kuitenkin lopettaa mainosten personoinnin kokonaan.[32]

Google kertoo myös avainsanojen väärintulkinnasta. Käyttäjä voi poistaa käy-

[3]https://support.google.com/googlenest/answer/7029281?hl=en

[4]https://safety.google/intl/fi/nest/

[5]https://support.google.com/googlenest/answer/7072285?hl=fi

tetyn äänidatan sanomalla "Avainsana, that wasn't for you". Google tarjoaa myös käyttäjille mahdollisuuden muokata älykaiuttimien kuulemisherkkyyttä, jonka tarkoituksena on vähentää mahdollisia avainsanan väärintulkintoja.[32]

Googlen tietoturvakäytännöllä on paljon samaa Amazonin käytännön kanssa. Google ilmoittaa Nest-laitteiden kuuluvan Google Vulnerability Reward Program -ohjelmaan. Ohjelman toimii samalla periaatteella kuin Amazonin VRP. Google lupaa rahallista palkitsemista ja julkista tunnustusta ihmisille, jotka löytävät haavoittuvuuksia Nest-laitteista. Palkkio maksetaan edellyttäen, että löytäjä säilyttää havaitsemansa haavoittuvuuden luottamuksellisena siihen asti, kunnes ongelma on korjattu. Googlella on myös henkilökuntaa, jonka tehtävänä on analysoida jokaisen laitteen laitteisto ja ohjelmisto ennen julkaisua. Riskejä ja turvallisuusvaaroja analysoidaan myös jatkuvasti laitteen ollessa markkinoilla. Lisäksi Nest-laitteissa on turvallinen käynnistys -ominaisuus. Google lupaa tärkeitä tietoturvapäivityksiä vähintään viiden vuoden ajan sen jälkeen, kun laite on ensimmäisen kerran saatavilla Yhdysvalloissa Google-kaupassa.[31]

Google pitää Google-tilit suojattuna esimerkiksi epäilyttävän toiminnan havaitsemisella, tietoturvatarkistuksilla ja kaksivaiheisen vahvistuksen avulla. Epäilyttävän toiminnan havaitseminen lähettää käyttäjille ilmoituksia, kun Google havaitsee epäilyttävää toimintaa tililläsi. Epäilyttävä toiminta voi olla esimerkiksi epätavallinen kirjautumislaite tai -sijainti tai kriittisten tietojen muuttaminen. Tietoruvatarkistuksella käyttäjä voi tarkastella Google-tilinsä tietoturvaa ja esimerkiksi hallinnoida Googlen tallentamia salasanoja. Google myös antaa käyttäjille vinkkejä koskien heidän tiliensä tietoturvaa. Kaksivaiheinen vahvistus vahvistaa Google-tilin tietoturvaa. Käyttäjä voi esimerkiksi valita saavansa älypuhelimeensa koodin, kun joku yrittää kirjautua hänen Google-tililleen.[31]

4.3 Apple HomePod

Apple liittyi älykaiutinmarkkinoille vuonna 2018, kun he julkaisivat HomePod-älykaiuttimen [33]. Applella on julkaissut Googleen ja Amazoniin verrattuna vähiten älykaiuttimia. Julkaistut HomePod-mallit ovat: 1st Generation Homepod (2018), HomePod Mini (2020) ja 2nd Generation HomePod (2023)[6]. Ensimmäinen HomePod on jo poistunut myynnistä Applen sivuilta[7]. Apple HomePod vaatii käyttäjältä Apple ID:n.

Applen sivuilta löytää kompaktin tekstin HomePod-laitteiden yksityisyydestä ja tietoturvasta. Sivulla esimerkiksi ohjeistetaan, miten käyttäjä voi estää kaiutinta kuuntelemasta. Apple myös kehottaa poistamaan HomePod-laitteen Apple Home -sovelluksesta ennen laitteesta luopumista. Sivulla on myös linkki toiselle sivulle, josta voi perehtyä tarkemmin Sirin ja HomePod-kaiuttimen yksityisyyteen ja tietoturvaan[8].[34]

Applen mukaan käyttäjän äänidata voidaan käsitellä paikallisesti tai Applen pilvessä. Jos äänidata käsitellään paikallisesti, ilmoitetaan siitä Sirin asetuksissa. Apple myös huomauttaa, että käyttäjän äänidataa ei käytetä mainostamiseen, mutta Sirin parantamiseen sitä voidaan käyttää. Kun äänidataa lähetetään pilveen, sitä ei yhdistetä käyttäjän Apple ID:hen, vaan käsitellään se Applen mukaan anonyymisti. Apple antaa myös käyttäjälle mahdollisuuden poistaa Sirin historian. [34]

Käyttäjästä lähetetään merkittävä määrä muuta tietoa Applelle, kun hän käyttää Siriä. Apple kertoo, että laite lähettää Applelle esimerkiksi seuraavat tiedot: Käyttäjän mahdollisesti määritettyjen yhteystietojen nimet, lempinimet ja suhteet, käyttäjän kuuntelema musiikki ja podcastit, käyttäjän ja Family Sharing -jäsenten laitteiden nimet sekä käyttäjän määrittämien hälytysten nimet ja ihmisten nimet valokuvissa. [34]

[6]https://support.apple.com/en-us/101609

[7]https://www.apple.com/homepod/

[8]https://www.apple.com/legal/privacy/data/en/ask-siri-dictation/

Applella on myös oma ohjelma, jonka avulla ihmiset voivat ilmoittaa Applelle mahdollisista tietoturvauhkista. The Apple Security Bounty Program toimii samalla periaatteella kuin Googlen ja Amazonin ohjelmat. Applen laitteissa on myös turvallinen käynnistys -ominaisuus.[34][35]

4.4 Vertailua

Edellä mainittujen laitevalmistajien, Amazonin, Googlen ja Applen, älykaiuttimien yksityisyydensuojaan ja tietoturvakäytäntöihin syventyminen paljasti pääosin samankaltaisia lähestymistapoja. Jokainen valmistaja tarjoaa oman ohjelmansa, kuten Amazon Vulnerability Research Program, Google Vulnerability Research Program ja The Apple Security Bounty Program, jotka kannustavat käyttäjiä ilmoittamaan mahdollisista tietoturvauhkista. Lisäksi jokaisessa laitteessa on turvallinen käynnistys -ominaisuus, joka vahvistaa laitteen ohjelmiston autenttisuuden ja lisää sen turvallisuutta.

Jokainen valmistaja kertoo käyttäjän mahdollisuuksista hallita äänidataansa. Jokainen tarjoaa käyttäjälle mahdollisuuden poistaa äänidataa, ja äänidatan käsittely paikallisesti on mahdollista kaikilla kolmella valmistajalla. Verkkosivuja tutkiessa ilmeni, että Apple on ainut laitevalmistaja, joka kertoo, että he eivät jaa äänidataa kolmansille osapuolille [36].

Käyttäjän näkökulmasta Amazonin ja Googlen sivut erottuivat helppolukuisuudellaan ja kattavalta tiedonmäärältään. Toisin kuin kilpailijoilla, Applella ei ollut erillistä sivua, jossa vastattiin käyttäjien yleisimpiin kysymyksiin. Apple HomePod -kaiuttimen yksityisyys- ja tietoturvasivu oli suppeampi verrattuna kilpailijoiden sivuihin, ja se ohjasi käyttäjät toiselle sivulle lisätietoja varten. Applella teknisemmät tiedot olivat haastavammin lähestyttäviä ja vaikeammin ymmärrettäviä verrattuna kilpailijoihin, joilla tekniset tiedot oli selitetty selkeästi ja käyttäjäystävällisesti. Tämä saattaa vaikuttaa käyttäjien kokemukseen ja ymmärrykseen laitteiden

yksityisyys- ja tietoturvatoimenpiteistä. Vaikka kaikilla valmistajilla on vahvat turvallisuuskäytännöt, käyttäjien ymmärryksen kannalta on tärkeää, että tekniset tiedot esitetään selkeästi ja helposti lähestyttävästi. Jatkuvan käyttäjäystävällisen tiedotuksen avulla kaikki kolme laitevalmistajaa voivat edelleen vahvistaa käyttäjiensä luottamusta älykaiuttimiensa yksityisyys- ja tietoturvatoimiin.

5 Yhteenveto

Älykaiuttimet ovat puheentunnistusta hyödyntäviä laitteita. Kyky kommunikoida laitteen kanssa äänikomennoilla on käytännöllistä ja nopeaa. Käyttäjä voi esimerkiksi toistaa musiikkia, tarkistaa sääennusteita ja hallita kodin älylaitteita. Älykaiuttimet tuovat mukanaan monia etuja ja mukavuuksia, mutta samalla herättävät myös huolia tietoturvasta ja yksityisyydestä.

Tässä tutkielmassa tutkittiin älykaiuttimiin liittyviä tietoturva- ja yksityisyyshuolia. Tutkielmassa myös määriteltiin älykaiuttimen ekosysteemi ja viitemalli. Näitä käytettiin tukena, kun perehdyttiin mahdollisiin tietoturvariskeihin ja niiden ehkäisykeinoihin. Yksityisyyshuolia kartoitettiin kolmen tekijän kautta, jotka olivat puheentunnistus, älykaiuttimen sijainti ja kolmannen osapuolen sovellukset. Lisäksi vertailtiin kolmen suurimman laitevalmistajan tietoturvaselosteita ja yksityisyydensuojia. Tutkielman ensimmäisen tutkimuskysymyksen tavoitteena oli selvittää mahdollisia tietoturva- ja yksityisyyshuolia sekä määrittää niiden merkittävyys kuluttajanäkökulmasta. Toisen tutkimuskysymyksen tavoitteena oli tutustua johtavien laitevalmistajien tietoturva- ja yksityisyyspolitiikkaan.

Tietoturvallisia uhkia älykaiuttimelle on jokaisella viitemallin tasolla. Laitevalmistajat kuitenkin esittelevät perusteellisia tapoja ennaltaehkäistä näitä. Keskeisimmät yksityisyyshuolet olivat puheentunnistus ja datankeruu. Jatkuvasti kuunteleva laite sijoittuu käyttäjien kotiin ja kerää äänidataa laitteen käyttäjiltä. Valmistajien sivuilta löytyy tietoa datakeruun keinosta ja käyttötarkoituksista. Lisäksi sivuilta

löytyy ohjeita käyttäjille, joissa esimerkiksi neuvotaan miten he voivat hallita omaa dataansa. Käyttäjänäkökulmasta yksityisyyshuolet ovat merkittävämpiä kuin tietoturvariskit.

Amazon, Google ja Apple tarjoavat kattavat verkkosivut tietoturvasta ja yksityisyydestä. Kaikki kolme tarjoavat omat ohjelmansa tietoturvariskien raportoinnille. Kaikkien sivuilta myös löytyi ohjeita käyttäjän äänidatan hallitsemiseksi. Amazonin ja Googlen verkkosivut olivat käyttäjäystävällisempiä kuin Applen verkkosivut. Esimerkiksi ymmärrettävyyden kannalta Applen sivut olivat haastavampaa luettavaa. On tärkeää, että käyttäjät ymmärtävät luettavansa valmistajien verkkosivuilta.

Mahdollisia jatkotutkimuksia voisi kohdistaa älykaiuttimien tietoturvan, yksityisyyden ja käytettävyyden tasapainottamiseen. On tärkeää taata käyttäjälle tietoturvallinen ja mahdollisimman yksityinen käyttökokemus. Haastavammaksi tässä yhtälössä ilmeni yksityisyyden ja käytettävyyden tasapainottaminen, koska datankeruulta ei voida välttyä ja puheentunnistus herättää huolia.

Kokonaisuudessaan tässä tutkielmassa kartoitettiin älykaiuttimiin liittyviä tietoturva- ja yksityisyyshuolia sekä tarkasteltiin merkittävien valmistajien verkkosivuja. Vaikka tietoturvallisia riskejä on olemassa, niihin on olemassa ehkäisykeinoja. Yksityisyyshuolia esiintyy puheentunnistuksen ja datankäytön osalta. Valmistajien verkkosivuilta löytyy runsaasti tietoa, mutta tekstistä voisi tehdä lähestyttävämpää ja käyttäjäystävälisempää.

Lähdeluettelo

[1] Y.-l. Liu, L. Huang, W. Yan, X. Wang ja R. Zhang, "Privacy in AI and the IoT: The privacy concerns of smart speaker users and the Personal Information Protection Law in China", Telecommunications Policy, vol. 46, nro 7, s. 102 334, 2022, ISSN: 0308-5961. DOI: https://doi.org/10.1016/j.telpol.2022.102334. url: https://www.sciencedirect.com/science/article/pii/S0308596122000362.

[2] Y. Park, H. Choi, S. Cho ja Y.-G. Kim, "Security Analysis of Smart Speaker: Security Attacks and Mitigation", Computers, Materials & Continua, vol. 62, nro 3, s. 1075–1090, 2019, ISSN: 1546-2226. DOI: 10.32604/cmc.2019.08520. url: http://www.techscience.com/cmc/v61n3/35289.

[3] X. Liu, A. Li, X. Fu, B. Luo, X. Du ja M. Guizani, "Understanding Digital Forensic Characteristics of Smart Speaker Ecosystems", teoksessa 2021 IEEE Global Commu 2021, s. 1–6. DOI: 10.1109/GLOBECOM46510.2021.9685816.

[4] A. H. Alhamedi, V. Snasel, H. M. Aldosari ja A. Abraham, "Internet of things communication reference model", teoksessa 2014 6th International Conference on Comput 2014, s. 61–66. DOI: 10.1109/CASoN.2014.6920423.

[5] G. Surman, "Understanding Security Using the OSI Model", 2002. url: https://www.sans.org/white-papers/377/.

[6] J. Lau, B. Zimmerman ja F. Schaub, "Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-Seeking Behaviors with Smart Speakers",

Proc. ACM Hum.-Comput. Interact., vol. 2, nro CSCW, s. 31, 2018. DOI: 10.1145/3274371. url: https://dl-acm-org.ezproxy.utu.fi/doi/10.1145/3274371.

[7] H. Mun, H. Lee, S. Kim ja Y. Lee, "A Smart Speaker Performance Measurement Tool", teoksessa Proceedings of the 35th Annual ACM Symposium on Applied Com sarja SAC '20, Brno, Czech Republic: Association for Computing Machinery, 2020, s. 755–762, ISBN: 9781450368667. DOI: 10.1145/3341105.3373990. url: https://doi-org.ezproxy.utu.fi/10.1145/3341105.3373990.

[8] M. B. Hoy, "Alexa, Siri, Cortana, and More: An Introduction to Voice Assistants", Medical Reference Services Quarterly, vol. 37, nro 1, s. 81–88, 2018, PMID: 29327988. DOI: 10.1080/02763869.2018.1404391. eprint: https://doi.org/10.1080/02763869.2018.1404391. url: https://doi.org/10.1080/02763869.2018.1404391.

[9] R. Maji, A. Biswas ja R. Chaki, "A Look into the Vulnerability of Voice Assisted IoT", teoksessa Computer Information Systems and Industrial Management, K. Saeed ja Dvorsk, toim., Cham: Springer International Publishing, 2022, s. 49–62, ISBN: 978-3-031-10539-5.

[10] G. Zhang, C. Yan, X. Ji, T. Zhang, T. Zhang ja W. Xu, "DolphinAttack: Inaudible Voice Commands", teoksessa Proceedings of the 2017 ACM SIGSAC Conference on sarja CCS '17, Dallas, Texas, USA: Association for Computing Machinery, 2017, s. 103–117, ISBN: 9781450349468. DOI: 10.1145/3133956.3134052. url: https://doi.org/10.1145/3133956.3134052.

[11] A. Hussain, N. Abughanam, J. Qadir ja A. Mohamed, "Jamming Detection in IoT Wireless Networks: An Edge-AI Based Approach", teoksessa Proceedings of the 12th I sarja IoT '22, Delft, Netherlands: Association for Computing Machinery, 2023,

s. 57–64, ISBN: 9781450396653. DOI: 10.1145/3567445.3567456. url: https://doi.org/10.1145/3567445.3567456.

[12] A. Mallik, "MAN-IN-THE-MIDDLE-ATTACK: UNDERSTANDING IN SIMPLE WORDS", vol. 2, 2018. url: https://jurnal.ar-raniry.ac.id/index.php/cyberspace/article/view/3453.

[13] Y. Lit, S. Kim ja E. Sy, "A Survey on Amazon Alexa Attack Surfaces", teoksessa 2021 IEEE 18th Annual Consumer Communications Networking Conference (CCNC) 2021, s. 1–7. DOI: 10.1109/CCNC49032.2021.9369553.

[14] M. Khawla ja M. Tomader, "A Survey on the Security of Smart Homes: Issues and Solutions", sarja ICSDE'18, Rabat, Morocco: Association for Computing Machinery, 2018, s. 81–87, ISBN: 9781450365079. DOI: 10.1145/3289100.3289114. url: https://doi.org/10.1145/3289100.3289114.

[15] G. Hu, "On Password Strength: A Survey and Analysis", teoksessa Software Engineering, A R. Lee, toim. Cham: Springer International Publishing, 2018, s. 165–186, ISBN: 978-3-319-62048-0. DOI: 10.1007/978-3-319-62048-0_12. url: https://doi.org/10.1007/978-3-319-62048-0_12.

[16] N. Meng, D. Keküllüoğlu ja K. Vaniea, "Owning and Sharing: Privacy Perceptions of Smart Speaker Users", Proc. ACM Hum.-Comput. Interact., vol. 5, nro CSCW1, huhtikuu 2021. DOI: 10.1145/3449119. url: https://doi-org.ezproxy.utu.fi/10.1145/3449119.

[17] N. Abdi, K. M. Ramokapane ja J. M. Such, "More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants", teoksessa Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019), Santa Clara, CA: USENIX Association, elokuu 2019, s. 451–466, ISBN: 978-1-939133-05-2. url: https://www.usenix.org/conference/soups2019/presentation/abdi.

[18] Y. Huang, B. Obada-Obieh ja K. (Beznosov, "Amazon vs. My Brother: How Users of Shared Smart Speakers Perceive and Cope with Privacy Risks", sarja CHI '20, Honolulu, HI, USA: Association for Computing Machinery, 2020, s. 1–13, ISBN: 9781450367080. DOI: 10.1145/3313831.3376529. url: https://doi.org/10.1145/3313831.3376529.

[19] M. Tabassum, T. Kosinski ja H. R. Lipford, ""I don't own the data": End User Perceptions of Smart Home Device Data Practices and Risks", teoksessa Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019), Santa Clara, CA: USENIX Association, elokuu 2019, s. 435–450, ISBN: 978-1-939133-05-2. url: https://www.usenix.org/conference/soups2019/presentation/tabassum.

[20] E. Zeng, S. Mare ja F. Roesner, "End User Security and Privacy Concerns with Smart Homes", teoksessa Thirteenth Symposium on Usable Privacy and Security (SOUPS Santa Clara, CA: USENIX Association, heinäkuu 2017, s. 65–80, ISBN: 978-1-931971-39-3. url: https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng.

[21] S. Zheng, N. Apthorpe, M. Chetty ja N. Feamster, "User Perceptions of Smart Home IoT Privacy", Proc. ACM Hum.-Comput. Interact., vol. 2, nro CSCW, marraskuu 2018. DOI: 10.1145/3274469. url: https://doi.org/10.1145/3274469.

[22] V. Zimmermann, M. Bennighof, M. Edel, O. Hofmann, J. Jung ja M. von Wick, "'Home, Smart Home' – Exploring End Users' Mental Models of Smart Homes", teoksessa Mensch und Computer 2018 - Workshopband, Bonn: Gesellschaft für Informatik e.V., 2018. DOI: 10.18420/muc2018-ws08-0539.

[23] "The Infinite Dial 2023 from Edison Research with Amazon Music, Wondery, and ART19", maaliskuu 2023. url: https://www.edisonresearch.com/

infinite-dial-2023-from-edison-research-with-amazon-music-wondery-and-art19/.

[24] G. Chalhoub ja I. Flechais, ""Alexa, Are You Spying on Me?": Exploring the Effect of User Experience on the Security and Privacy of Smart Speaker Users", teoksessa HCI for Cybersecurity, Privacy and Trust, A. Moallem, toim., Cham: Springer International Publishing, 2020, s. 305–325.

[25] A. S. Alrumayh, S. M. Lehman ja C. C. Tan, "Understanding and Mitigating Privacy Leaks from Third-Party Smart Speaker Apps", teoksessa 2021 IEEE Conference o 2021, s. 1–9. DOI: 10.1109/CNS53000.2021.9705042.

[26] C. Welch, "Amazon just surprised everyone with a crazy speaker that talks to you", 2014. url: https://www.theverge.com/2014/11/6/7167793/amazon-echo-speaker-announced.

[27] Amazon, url: https://www.amazon.com/gp/help/customer/display.html?nodeId=GVP69FUJ48X9DK8V.

[28] Amazon, url: https://www.amazon.com/b/?node=23638098011.

[29] S. Kovach, "Google unveils its newest major product: the Google Home speaker", 2016. url: https://www.businessinsider.com/google-home-announced-price-release-date-2016-10?r=US&IR=T&utm_source=copy-link&utm_medium=referral&utm_content=topbar.

[30] Google, url: https://blog.google/inside-google/company-announcements/nest-join-forces-googles-hardware-team/.

[31] Google, url: https://safety.google/intl/fi/nest/.

[32] Google, url: https://support.google.com/googlenest/answer/7072285?hl=fi.

[33] Apple, url: https://www.apple.com/newsroom/2018/01/homepod-arrives-february-9-available-to-order-this-friday/.

[34] Apple, url: https://support.apple.com/guide/homepod/privacy-and-security-apd99ee29027/homepod.

[35] Apple. url: https://security.apple.com/bounty.

[36] S. Alghamdi ja S. Furnell, "Assessing Security and Privacy Insights for Smart Home Users.", teoksessa ICISSP, 2023, s. 592–599.