TURUN YLIOPISTO
Kauppakorkeakoulu

Puettavan teknologian datan kyberturvallisuus ja tietosuojahaasteet

Tietojärjestelmätieteen kandidaatintutkielma

Laatija(t):
Amanda Ruuhijärvi

Ohjaaja(t):
FT Samuli Laato

15.12.2024
Turku

Kanditutkielma

Oppiaine: Tietojärjestelmätiede
Tekijä(t): Amanda Ruuhijärvi
Otsikko: Puettavan teknologian datan kyberturvallisuus ja tietosuojahaasteet
Ohjaaja(t): FT Samuli Laato
Sivumäärä: 32 sivua
Päivämäärä: 15.12.2024

Puettavan teknologian, kuten älykellojen ja aktiivisuusmittareiden, yleistyminen tuo mukanaan merkittäviä kyberturvallisuus- ja tietosuojahaasteita. Nämä laitteet keräävät ja siirtävät suuria määriä arkaluonteisia tietoja, kuten terveystietoja ja sijaintitietoja, jotka voivat joutua kyberhyökkäysten ja tietovuotojen kohteeksi. Tämä kandidaatintutkielma tarkastelee, millaisia uhkia puettavan teknologian laitteisiin kohdistuu, miten nämä uhat voivat vaikuttaa käyttäjien yksityisyyteen ja turvallisuuteen sekä mitä toimia uhkien ehkäisemiseksi ja hallitsemiseksi tulisi toteuttaa.

Tutkielma on toteutettu kirjallisuuskatsauksena, ja aineistona on käytetty aihetta käsitteleviä tieteellisiä artikkeleita ja muuta aiheeseen liittyvää kirjallisuutta, kuten markkina-analyysejä ja uutisartikkeleita. Tutkielma tarjoaa yleiskatsauksen puettavaan teknologiaan kohdistuvista monenlaisista uhista, kuten tietomurroista, tietovuodoista ja tietojen manipuloinnista, jotka voivat vaarantaa käyttäjien yksityisyyden sekä fyysisen turvallisuuden. Lisäksi tutkielmassa nostetaan esiin lainsäädännön ja teknologisten ratkaisujen merkitys turvallisuuden takaamiseksi. Esimerkkitapauksena käytetty Fitbit tuo esille tietoturvapuutteita, jotka ovat tyypillisiä myös muille puettaville laitteille. Fitbitin tapaus konkretisoi tutkielmassa käsitellyt uhat ja tarjoaa käytännön esimerkin aiheesta, samalla havainnollistaen laitteiden käyttöön liittyviä riskejä ja niiden mahdollisia seurauksia. Lisäksi Fitbitin tapaus auttaa ymmärtämään, miten tietoturvahaavoittuvuudet voivat vaikuttaa käyttäjien yksityisyyteen ja turvallisuuteen, sekä millaisia toimenpiteitä tarvitaan näiden riskien hallitsemiseksi. Fitbitin tarkastelu tarjoaa tietoa, jota voidaan hyödyntää laajemmin puettavan teknologian kehityksessä ja tietoturvakäytäntöjen parantamisessa.

Kirjallisuuskatsauksen löydösten perusteella puettavan teknologian turvallisuutta voidaan parantaa esimerkiksi vahvempien salausmenetelmien, tiukempien todennuskäytäntöjen ja käyttäjätietoisuuden lisäämisen avulla. Näitä menetelmiä voidaan kohdistaa eri kohderyhmille, kuten valmistajille ja loppukäyttäjille. Valmistajille suunnattuja suosituksia ovat esimerkiksi vahvempien suojausprotokollien kehittäminen, ohjelmistopäivitysten tarjoaminen ja tietoturvan huomioiminen jo suunnitteluvaiheessa. Loppukäyttäjille suunnattuja keinoja ovat puolestaan käyttäjätietoisuuden lisääminen sekä selkeät ohjeet turvallisten käyttöasetusten valitsemiseksi. Lisäksi puettavan teknologian tietosuoja- sekä kyberturvallisuusasioiden sääntelyn kehittäminen on keskeisessä asemassa yksityisyyden suojaamisessa ja riskien hallinnassa. Tutkielma tarjoaa tietoa puettavan teknologian käyttäjille ja kehittäjille, ja se korostaa turvallisuusnäkökulmien tärkeyttä teknologian suunnittelussa ja käytössä. Puettavan teknologian nopea kehitys edellyttää ennakoivia toimenpiteitä, jotta yksilöiden yksityisyyttä voidaan suojata teknologian laajentuessa ja sen käyttökohteiden monipuolistuessa. Tämä tarkoittaa esimerkiksi sitä, että valmistajien tulee kehittää tietoturvamekanismeja, jotka mukautuvat uusiin uhkiin, sekä varmistaa käyttäjien yksityisyys lainsäädännön ja teknisten ratkaisujen avulla. Ennakoivat toimenpiteet, kuten riskianalyysi ja tietoturvapäivitykset, ovat keskeisiä keinoja ongelmien ehkäisyssä.

Avainsanat: Puettava teknologia, kyberturvallisuus, tietosuoja

SISÄLLYS

KUVIOT

TAULUKOT

1 Johdanto

Puettavalla teknologialla tarkoitetaan vaatteita, asusteita ja koruja, joihin on digitaalisen teknologian avulla lisätty esimerkiksi viestintään, seurantaan tai lämmittävyyteen liittyviä ominaisuuksia. Digitaalisella teknologialla tarkoitetaan esimerkiksi digitaalisia laitteita tai elektrodeja sisältäviä älytekstiilejä. Tähän kuuluvat esimerkiksi älykellot ja aktiivisuusmittarit, jotka mahdollistavat tietojen keräämisen ja jakamisen muiden laitteiden, kuten älypuhelinten ja digitaalisten sovellusten, kanssa. (Quinn, 2013). Puettavan teknologian laitteita ovat myös esimerkiksi langattomat kuulokkeet, älykkäät sydämentahdistimet, piilolinssit, sormukset tai silmälasit.

Puettava teknologia on yleistynyt merkittävästi viime aikoina. Keskimäärin 28% suomalaisista ihmisistä käyttää päivittäin jotakin puettavan teknologian laitetta, jolla pystytään seuraamaan terveydentilaan liittyviä yksityiskohtia, kuten esimerkiksi sydämensykettä ja unen laatua. (Kyytsönen et al, 2023.) Vuonna 2021 älykellojen liikevaihto on ollut 22,46 miljardia Yhdysvaltain dollaria ja sen ennustetaan kasvavan jopa 118,16 miljardiin dollariin vuoteen 2028 mennessä (Grand View Research, 2022).

Puettavat laitteet tarjoavat käyttäjilleen lukuisia hyötyjä (Mills et al., 2016). Puettava teknologia on antanut maailman parhaille urheilijoille mahdollisuuden optimoida urheilutuloksensa ja antanut kaikille mahdollisuuden elää parempaa elämää käyttämällä biotietoja terveyspäätösten tukena (Andjelic et al. 2022, Mills et al., 2016). Ne ovat henkilökohtaisimpia ja ainutlaatuisimpia laitteita. Puettavan teknologian laitteista henkilökohtaisia ja ainutlaatuisia tekee se, että ne on suunniteltu hyödyttämään ainoastaan yksittäistä käyttäjää esimerkiksi mukautumalla käyttäjän anatomisiin ominaisuuksiin. Kuitenkin ainutlaatuisuus tuo myös mukanaan uusia turvallisuusongelmia, kuten mahdollisuuden vaarantaa käyttäjien tietoja ja jopa fyysisesti vahingoittaa heitä. Älykello voidaan esimerkiksi ohjelmoida lähettämään sarja ärsyttäviä, mutta merkityksettömiä impulsseja ilman syytä. Diabeetikon puettavan älylaitteen hakkerointi väärien lukemien antamiseksi voi puolestaan johtaa siihen, että käyttäjä ei saa varoitussignaaleja tai ylireagoi liioiteltuihin glukoositasoihin. Tämä voi aiheuttaa vakavia seurauksia ja jopa osoittautua hengenvaaralliseksi. (Mills et al., 2016.)

Aktiivisuusmittarit, jotka seuraavat esimerkiksi sykettä, askelmääriä ja pulssia, nähdään yleensä harmittomina käyttäjän yksityisyydelle. On kuitenkin todennäköistä, että käyttäjät eivät ole tietoisia siitä, miten kolmannet osapuolet voivat väärinkäyttää tällaisia tietoja tai millaisia mahdollisia yksityisyysongelmia syntyy, kun tietoja kerätään pitkäaikaisesti tai yhdistetään muihin tietoihin. (Motti & Caine, 2015.) Kaikkeen teknologiaan liittyy riskejä kerätyn datan tietoturvan ja

kyberturvallisuuden osalta. Puettavat laitteet voivat vaarantaa käyttäjien henkilötietoja tietosuojan näkökulmasta. (Ziccardi, 2020.) Puettavan teknologian laitteet keräävät usein arkaluonteista tietoa, kuten tietoa sydämen sykkeestä, askelmäärästä, unikäyttäytymisestä ja sijainnista. Näiden tietojen turvallisuus on tärkeää, sillä jos niitä käsitellään huolimattomasti, voidaan tietoja käyttää epätoivotulla tavalla. Lisäksi, koska puettavan teknologian laitteet ovat osa laajempaa esineiden internetiä (IoT), ne voivat olla alttiita kyberhyökkäyksille, jotka voivat vaarantaa yksilöiden yksityisyyden ja turvallisuuden. (Satria et al., 2022.)

Esimerkkinä kyberhyökkäyksistä voidaan mainita psykoterapiakeskus Vastaamo, joka joutui kyberhyökkäyksen kohteeksi vuonna 2020. Hyökkäyksessä saatiin haltuun Vastaamon arkaluonteiset ja henkilökohtaiset potilastiedot, joita käytettiin kiristämiseen. Hyökkääjä uhkasi julkaista päivittäin 100 ihmisen tietoja internetissä, ellei hänelle maksettaisi 450 000 euroa bitcoineina. Hyökkääjä ehti julkaista useita arkaluonteisia tietoja Tor-verkkoon. (Heikkilä & Cerulus, 2020.) Vastaamon tapaus osoittaa kuinka vakavia seurauksia arkaluonteisten tietojen joutumisella vääriin käsiin voi olla. Vastaava kyberhyökkäys voisi kohdistua puettavan teknologian laitteisiin, kuten älykelloihin, jotka keräävät ja tallentavat runsaasti yksityistä tietoa, kuten käyttäjän terveystiedot, sijaintihistorian, uni- ja aktiivisuusraportit sekä mahdollisesti biometriset tiedot. (Arias et al., 2015; Banerjee et al., 2018.) Koska älykellojen keräämää dataa siirretään ja tallennetaan usein pilvipalveluihin, hyökkäys voisi tapahtua esimerkiksi murtautumalla näihin pilvipalveluihin ja varastamalla sieltä laajan määrän henkilökohtaisia tietoja (Ioannidou & Sklavos, 2021).

Tiedot voivat päätyä kolmansille osapuolille myös ilman kyberhyökkäystä. Esimerkiksi sijaintipohjaisissa peleissä, kuten Pokémon GO:ssa, pelaajien liikkumista ja sijaintihistoriaa voidaan seurata, mikä mahdollistaa arkaluonteisten tietojen päätymisen muiden pelaajien tai haitallisten toimijoiden käsiin. Lisäksi yritykset voivat myydä anonymisoituja käyttäjätietoja kolmansille osapuolille, mikä voi johtaa tietojen yhdistelyyn ja paljastaa tietoja yksittäisten käyttäjien liikkeistä ja käyttäytymismalleista kaupallisiin tai haitallisiin tarkoituksiin (Rauti & Laato, 2024).

Puettavat laitteet mahdollistavat sekä yksilöiden, että heidän käyttäytymisensä ja ympäristönsä seurannan, mikä voi johtaa merkittäviin yksityisyyttä uhkaaviin riskeihin. Nämä ongelmat eivät kosketa ainoastaan yksittäistä käyttäjää, vaan myös yhteiskuntaa ja asiaan liittyviä organisaatioita, esimerkiksi silloin, kun kerättyjä tietoja käytetään väärin. Koska puettavien laitteiden käyttö on suhteellisen uutta, tämänkaltaisia vaikutuksia ei ole vielä täysin ymmärretty. (Motti & Caine, 2015.) Vaikka valmistajat ovat tietoisia tietosuoja- ja turvallisuusvaikutuksista, turvallisuus joko

laiminlyödään tai huomioidaan vasta jälkikäteen. Tämä johtuu usein lyhyistä markkinoille pääsyajoista ja kustannusten vähentämisestä, jotka ohjaavat laitteen suunnittelu- ja kehitysprosessia. (Arias et al., 2015.) Suurin osa markkinoilla olevista puettavista laitteista on esimerkiksi Applen ja Googlen kaltaisten jättiyritysten kehittämiä ja myymiä. Kulutusteknologiayritysten kasvava terveysdatan keruu tarjoaa niille merkittäviä taloudellisia ja poliittisia etuja, sillä ne voivat hyödyntää näitä tietoja markkinoinnissa ja mainonnassa. (Canali et al., 2022.) Tämän tutkielman tarkoituksena on perehtyä millaisia kyberturvallisuusuhkia ja tietosuojariskejä puettavaan teknologiaan kohdistuu ja miten nämä uhat voivat vaikuttaa käyttäjien yksityisyyteen. Tutkielmassa keskitytään puettaviin laitteisiin, jotka keräävät arkaluonteista tietoa käyttäjästään, kuten älykellot, aktiivisuusrannekkeet, sekä lääkinnälliseen tarkoitukseen käytettävät puettavat laitteet. Tutkielmassa pyritään sekä tunnistamaan ja kuvailemaan puettavan teknologian uhkia, että ymmärtämään, miten nämä uhat voivat vaikuttaa käyttäjiin sekä heidän yksityisyyteensä. Tutkielma auttaa puettavan teknologian käyttäjiä ymmärtämään millaisia uhkia teknologiaan kohdistuu vastaamalla seuraaviin kysymyksiin:

Millaisia kyberturvallisuusuhkia puettavaan teknologiaan kohdistuu?

Miten nämä uhat voivat vaikuttaa käyttäjiin?

Tutkielma koostuu viidestä luvusta: johdanto, kolme asialukua sekä pohdinta ja yhteenveto. Luvussa kaksi esitellään puettavan teknologian kyberturvallisuuteen ja tietosuojaan liittyvät yleisimmät ja suurimmat uhat sekä kerrotaan syitä uhille. Luvussa esitellään myös CIA-kolmio tietoturvan arviointikehyksenä ja sitä sovelletaan puettavaan teknologiaan. Luvussa kolme keskitytään siihen, millaisia konkreettisia seurauksia uhilla voi olla puettavan teknologian käyttäjiin. Luvussa neljä esitellään havainnollistavana esimerkkinä Case-esimerkki Fitbit-älykellon tietoturvaongelmista ja niiden seurauksista Lopuksi viimeinen luku kokoaa yhteen tutkielman keskeiset löydökset ja johtopäätökset. Luvussa pohditaan millaisia toimenpiteitä tarvitaan puettavan teknologian tietoturvan kehittämiseksi. Lisäksi luvussa esitellään myös tutkielman rajoitteet ja siinä pohditaan, millaisia tulevaisuuden tutkimusmahdollisuuksia aiheeseen on.

2 Millaisia kyberturvallisuusuhkia puettavaan teknologiaan kohdistuu?

Puettavan teknologian, kuten älykellojen ja aktiivisuusmittareiden, suosio on kasvanut suuresti viime vuosikymmenen aikana. Esimerkiksi DNA:n teettämän tutkimuksen mukaan älykellojen myynti kasvoi peräti 95 prosenttia vuosina 2019-2020 (Erkkilä, 2021). Viime vuosiin perustuvien ennusteiden mukaan markkinoiden odotetaan kasvavan noin 14,6% vuodessa, vuodesta 2023 vuoteen 2030 (Grand View Research, 2022). Näiden laitteiden avulla käyttäjät voivat seurata terveyteensä ja hyvinvointiinsa liittyviä tietoja, mutta samalla ne avaavat käyttäjille uudenlaisen uhkakentän. Puettavat laitteet keräävät ja siirtävät suuria määriä arkaluonteista tietoa, kuten terveystietoja, sijaintitietoja ja käyttäytymismalleja, mikä tekee niistä houkuttelevia kohteita hakkereille ja rikollisille. Tiedot kiinnostavat myös monia muita tahoja, jotka voivat hyödyntää dataa esimerkiksi kohdennettuun markkinointiin. Lisäksi suojaamattomat yhteydet ja heikot tietoturvakäytännöt voivat lisätä tietovuotojen ja muiden tietoturvaongelmien riskiä. Tässä luvussa tarkastellaan keskeisimpiä puettavan teknologian käyttöön liittyviä kyberturvallisuusuhkia ja niiden taustalla olevia tekijöitä.

Taulukko 1 tiivistää puettavaan teknologiaan liittyvät tietoturvauhat ja antaa niille määritelmät.

Uhka:	Kuvaus uhasta:	Lähde:
Kyberhyökkäykset	Kyberhyökkäykset ovat tietokoneiden välisiä hyökkäyksiä, joiden tavoitteena on heikentää järjestelmien tai tietojen luottamuksellisuutta, eheyttä ja/tai saatavuutta.	(Kim et al., 2012; Kshetri, 2013)
Käyttäjän tietojen väärinkäyttö	Käyttäjän tietojen väärinkäytöllä tarkoitetaan tilannetta, jossa henkilö, jolla on pääsy arkaluonteisiin tietoihin, käyttää tätä pääsyään sopimattomalla tavalla omiin tarkoituksiinsa.	(Shabtai et Al., 2014; Solove, 2006)
Epäluotettavat sovellukset	Epäluotettavat sovellukset ovat sovelluksia joilla ei ole takeita turvallisuudesta, alkuperästä tai käyttäytymisestä. Tällaiset sovellukset voivat potentiaalisesti suorittaa haitallisia toimintoja tai käyttää järjestelmän resursseja tavalla, joka voi vaarantaa tietoturvan tai yksityisyyden.	(Acharya & Raje, 2000; Felt et al., 2012)
Tietovuodot	Tietovuoto on luottamuksellisten tietojen tahallista tai tahatonta paljastumista luvattomille osapuolille.	(Cheng et Al., 2017; Riek & Böhme, 2018)

Taulukko 1 Puettavaan teknologiaan liittyvät tietoturvauhat

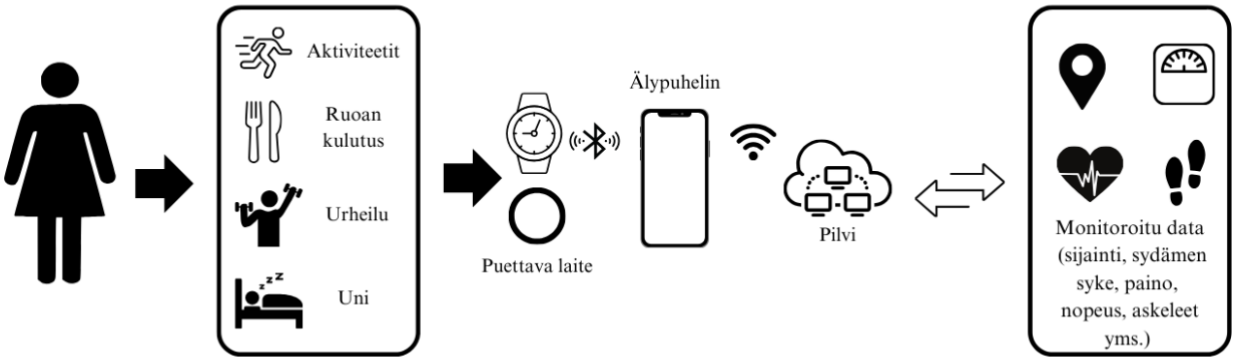
2.1 Kyberhyökkäykset

Puettavat laitteet ovat herkkiä samankaltaisille uhille, kuin muutkin laitteet, jotka ovat olleet houkuttavia kohteita ”hakkereilla” jo vuosikymmeniä (Ometov et al., 2017). Ne ovat olleet ja ovat alttiita kyberhyökkäyksille johtuen naiiveista suunnitteluratkaisuista ja puutteellisista tietoturvatoimenpiteistä. Huolestuttavasti tilanne on vielä pahempi puettavien lääkinnällisten laitteiden kohdalla.(Mohd et al., 2022.) Kaupalliset älyrannekkeet voivat paljastaa henkilökohtaisten tietojen lisäksi terveystietoja sekä laitteesta että palvelimelta johtuen laitteiden virheellisestä konfiguroinnista. Jos laitteen pariliitos on sallittu ilman todennusta, hyökkääjät voivat esimerkiksi hyödyntää tätä saadakseen käyttäjän terveystietoja. (Olabenjo & Makaroff, 2019.)

Suurin osa puettavista laitteista ovat alttiita kolmen tyyppisille hyökkäyksille. Yksi keskeisistä uhista on kuuntelu, joka tarkoittaa luvatonta reaaliaikaista luottamuksellisen viestinnän salakuuntelua. Toinen uhista on liikenteen analysointi, jossa seurataan puettavien laitteiden ja niihin liitettyjen laitteiden, sekä palvelimien välistä viestintää. Kolmas uhista on tietojen kerääminen, jolloin tietoja kerätään ja siirretään laitteen ja siihen liitetyn laitteen, usein älypuhelimen välillä. (Fúster et al., G. Lopez, 2022.) Näitä hyökkäyksiä voidaan tehdä hyödyntäen esimerkiksi älykellojen ja älylaitteiden välisiä langattomia yhteyksiä, kuten Bluetooth- tai puhelinverkkoyhteyksiä sekä pilvipalveluihin tallennettua dataa (Ometov et al., 2017). Jokainen nykyaikainen älypuhelin on varustettu Bluetooth- ja Wi-Fi-moduuleilla, joita tarvitaan yhteyksien muodostamiseen puettavien laitteiden ja niiden sovellusten välillä, mutta ne kärsivät silti monista haavoittuvuuksista. (Ioannidou & Sklavos, 2021.) Esimerkiksi käyttäjän laite voi muodostaa yhteyden väärään Wi-Fi-verkkoon, jolloin hyökkääjä voi siepata tai manipuloida tiedonsiirtoa (Ramezanpour et al., 2021). Mikäli tietoja lähetetään salaamattomana, ne ovat erittäin alttiita luvattomien tahojen sieppaamiselle siirron aikana, erityisesti suojaamattomissa verkoissa tai tilanteissa, joissa turvallista viestintäprotokollaa ei noudateta (Kantarcioglu & Clifton, 2005). Tällaisten haavoittuvuuksien vuoksi on suuri riski, että käyttäjien arkaluontoisia tietoja voi vuotaa ilman lupaa (Ioannidou & Sklavos, 2021).

Laitteen yksinkertainen hakkerointi voi aiheuttaa sen, että henkilö joko menettää kaikki tietonsa, ne varastetaan tai niitä muutetaan. Koska monet puettavat laitteet ovat yhteydessä käyttäjän muihin tietojärjestelmiin, kuten älypuhelimiin ja tietokoneisiin, niitä voidaan mahdollisesti myös käyttää porttina näihin laitteisiin tallennettuihin laajempiin tietoihin. Puettavaa laitetta voitaisiin myös käyttää käyttäjän sijainnin selvittämiseen tarkoituksena vahingoittaa häntä tai hänen laitteitaan tai murtautua hänen omaisuuteensa. (Mills et al., 2016.) Kuvio 1 havainnollistaa prosessia, jossa

puettavan laitteen käyttäjän aktiivisuutta seurataan ja tiedot välitetään älypuhelimeen sekä edelleen pilvipalveluun, josta ne palautetaan käyttäjälle helppolukuisessa muodossa älykellon näytölle tai älypuhelimeen.



Kuva 1 Puettavan laitteen seuranta- ja tiedonkeruuprosessi (mukaillen Webb, 2022)

Murtautumalla laitteen tietoturvaan ulkopuolinen taho voi saada runsaasti tietoa käyttäjän käyttäytymisestä. Vaihtoehtoisesti käyttäjän laitteen tietoja voidaan manipuloida välittämään virheellistä tietoa käyttäjän toiminnasta. Voidaan esimerkiksi antaa ymmärtää, että henkilö noudattaisi lääketieteellistä hoito-ohjelmaa, vaikka ei todellisuudessa niin tekisi tai johtaa lääkäriä määräämään lisälääkitystä, jota potilas ei tarvitse. Mikäli laitteen kertomia tietoja manipuloidaan, voi laite epäonnistua tehtävässään informoida käyttäjää. Esimerkiksi Saflet-älyranneke hälyttää muita henkilöitä käyttäjän maantieteellisestä sijainnista silloin, kun käyttäjä on yksin mahdollisesti vaarallisella alueella yöllä. Jos laite johtaisi signaalien vastaanottajat harhaan uskomaan, että käyttäjä on turvassa, vaikka hän ei ole, voisivat seuraukset olla vakavat. (Mills et al., 2016.)

2.2 Käyttäjien tietojen väärinkäyttö

Puettavat laitteet mahdollistavat yksilöiden, heidän käyttäytymisensä ja ympäristönsä tarkkailun, mikä voi johtaa merkittäviin yksityisyyden uhkiin ja riskeihin. Nämä ongelmat eivät vaikuta ainoastaan yksittäiseen käyttäjään, vaan myös yhteiskuntaan ja osallistuviin organisaatioihin, esimerkiksi silloin, kun kerättyjä tietoja käytetään väärin. (Kapoor et al. 2020.) Suurin

kyberturvallisuusriski liittyen puettaviin laitteisiin onkin henkilökohtaisten sekä tunnistettavien tietojen luvaton paljastuminen (Ometov et al., 2017).

Nykyään puettavia laitteita, erityisesti älykelloja, käytetään myös yritysympäristössä liiketoiminnan tehostamiseksi (Perera et al., 2015). Yritykset voivat käyttää niitä työntekijöiden yksityisyyden loukkaamiseen; työnantaja voi seurata työntekijöiden toimia ja lisäksi nähdä tietoja heidän terveydentilastansa. Näin arkaluonteiset tiedot voivat tulla ulkopuolisten saataville ja ne voivat näiden laitteiden kautta paljastua luvattomille henkilöille. (Siboni et al., 2016.) Organisaatiot, jotka sallivat puettavien laitteiden käytön työpaikalla, eivät välttämättä ole täysin tietoisia mahdollisista tietoturva-aukoista, joita työntekijöiden laitteet voivat aiheuttaa. Useimmat yritykset – jopa suuret organisaatiot, joilla on vakiintuneet turvallisuustoimenpiteet – eivät pidä näitä laitteita mahdollisina uhkina verkon turvallisuudelle. (Blow et al., 2020.)

Tulevaisuudessa useista eri lähteistä, kuten puettavista laitteista ja sähköisistä potilastiedoista, kerättyjä tietoja yhdistetään, jotta saadaan kattava kuva yksilön terveydentilasta (Montgomery et al., 2018). Monia käyttäjiä huolestuttaa se, että he eivät hallitse, mitä tietoja kerätään, milloin tietoja kerätään ja mihin niitä käytetään (Katurura & Cilliers, 2017). Vielä huolestuttavampi kysymys on käyttäjästä kerätyn datan omistajuus. Tällä hetkellä dataa ei omista käyttäjä itse, vaan puettavan laitteen valmistava yritys. Käyttäjä saa pääsyn vain yhteenvetoon omista tiedoistaan, kun taas raakadataa tiedoista voidaan myydä kolmansille osapuolille. (Piwek et al.., 2016.) Nämä kysymykset herättävät vakavia yksityisyyttä koskevia huolia puettavaa teknologiaa käyttävän yksilön kannalta (Katurura & Cilliers, 2017).

2.3 Epäluotettavat sovellukset

Sovellustasolla on tunnistettu useita merkittäviä turvallisuusongelmia, jotka vaikuttavat puettaviin laitteisiin liittyviin mobiilisovelluksiin, kuten haitallisen sisällön syöttäminen asiakkaille, puutteellinen istunnon hallinta, epäluotetun syötteen hyväksyminen, sivukanavien tietovuodot ja turvaton tiedon tallennus. Sivukanavat, joissa yksi sovellus lukee tietoja tilasta johon toinen sovellus pääsee käsiksi, ovat erityisen merkityksellisiä puettavien laitteiden kannalta. Silloin ohjelmointivirheet tai epävarmojen käyttöjärjestelmien ominaisuuksien pois päältä jättäminen sovelluksissa voi johtaa siihen, että arkaluonteiset tiedot päätyvät verkkovälimuisteihin, käyttöjärjestelmän yleisiin lokeihin, näyttökuviin ja tilapäiskansioihin. (Jain & Shanbhag, 2012.) Tällöin tiedot ovat haittaohjelmien tai puhelimen varastavan hyökkääjän ulottuvilla. Älykellojen sovellukset vaativat lupia sensorien, käyttäjäprofiilien ja Internet-yhteyden käyttöön. Nämä luvat eivät ole välttämättömiä monille mobiilisovelluksille, mutta ovat olennaisia terveys- ja

kuntosovelluksille sekä muille puettavien laitteiden sovelluksille niiden tehokkaan toiminnan takaamiseksi. Pääsy puettavien laitteiden tietoihin mahdollistaa haitallisten sovellusten pääsyn käyttäjän henkilökohtaisiin tietoihin. Lisäksi hyväntahtoisia sovelluksia voidaan hyödyntää hyökkäyksiin, jos ne lähettävät yksityisiä tietoja suojaamattomasti. (Olabenjo & Makaroff, 2019.) Koska puettavat sovellukset voivat sijaita joko puhelimessa, kellossa tai molemmissa ja kaikilla laitteilla on suora pääsy Internetiin, tietovuodot voivat tapahtua eri tavoin näiden laitteiden monipuolisten tiedonkeruu-, tallennus- ja siirtotapojen vuoksi. (Bouderhem, 2023.) Monilla puettavien laitteiden sovelluksilla on käyttöoikeusristiriita. Tämä mahdollistaa sen, että haitalliset sovellukset voivat pyytää lupaa päästä henkilötietoihin, joita ei tarvita itse sovelluksen toimintaan. Joissain tapauksissa käyttöoikeusristiriita puettavan laitteen ja sen mobiilisovelluksen välillä voi johtaa siihen, että henkilökohtaisia tietoja paljastetaan mobiililaitteen kautta ilman käyttäjän asianmukaista suostumusta. (Olabenjo & Makaroff, 2019.)

Sovellukset keräävät usein ylimääräistä tai käyttötarkoitukseensa suoraan liittymätöntä tietoa. Ne eivät myöskään aina tiedota käyttäjille selkeästi, millaista arkaluonteista tietoa kerätään tai tarjoa mahdollisuutta kieltäytyä tietojen keräämisestä. Tämä voi johtua siitä, että valmistaja pyrkii jälleenmyymään tiedot ja siksi kerää mahdollisimman paljon informaatiota. Tällöin vuotaneet tiedot eivät rajoitu pelkästään sovelluksen valmistajille, vaan voivat päätyä kenen tahansa haltuun, joka ne saa käsiinsä. (Kolias et al., 2016.) Chauhan et al. (2016) testasivat useita puettavien laitteiden sovelluksia tietovuotojen paljastamiseksi. He keskittyivät liikenteen tarkkailuun ja havaitsivat, että ainutlaatuisia tunnisteita, sijaintitietoja, tunnistetietoja ja terveystietoja siirretään internetiin. Vuonna 2016 noin 4–11 % sovelluksista lähetti älykelloihin liittyviä käyttäjätoimintoja kolmansille osapuolille, joista Google Analytics oli yleisin. Tämä johtuu siitä, että seurantarajapinnat eivät vaadi erityisiä lupia sen suhteen, millaista tietoa sovellusten tulisi lähettää. (Chauhan et al., 2016.) Aiheesta kouluttamattomat käyttäjät voivat helposti joutua sosiaalisen manipuloinnin ja muiden ja muiden puettavan teknologian haavoittuvuuksia hyödyntävien kyberhyökkäysten uhreiksi (Blow et al., 2020).

2.4 Tietosuoja

Puettavan teknologian laitteiden henkilökohtaisuus ja intiimiys tarjoaa valtavasti erilaisia hyötyjä yksilöille ja organisaatioille. Siitä johtuen on myös niiden turvallisuus kriittisempää. (Mills et al., 2016.) Puettavien laitteiden markkinoiden nopea kasvu edistää teknologista kehitystä, mutta luo myös riskin, että niiden tuotanto kasvaa ilman asianmukaista valvontaa ja sääntelyä, jota tarvitaan yksityisyyden ja turvallisuuden riittävän tason varmistamiseksi. Puutteellinen tai tehoton valvonta

voi johtaa tietoturvaltaan epävakaiden tuotteiden julkaisuun, joissa käytettävyyttä painotetaan turvallisuuden kustannuksella. (Fúster et al., 2022.)

Puettavan teknologian kehittäjät pyrkivät jatkuvasti luomaan entistä kehittyneempiä ja tehokkaampia laitteita, mikä syventää kuilua teknologian kehityksen ja sitä säätelevän lainsäädännön välillä (Mills et al., 2016). Näiden laitteiden odotetaan olevan kysyttyjä markkinoilla, ja valmistajat pyrkivät optimoimaan niiden komponentteja kustannusten vähentämiseksi keskittyen tarjoamaan vain vähimmäistoiminnallisuuden ja jättäen huomiotta perustavanlaatuisia turvallisuustarpeita (Silva-Trujillo et al., 2023.; Chang et al., 2019). Ometov et al. (2021) ovat todenneet tutkimuksessaan, kuinka muun muassa kannettavuus, langattomat yhteydet, energiatehokkuus ja kehittynyt näyttöteknologia on yhdistetty luomaan huipputason puettavia laitteita. Tämä on kuitenkin johtanut siihen, että vahvojen tietoturvaratkaisujen toteuttaminen on muuttunut entistä haastavammaksi (Ometov et al., 2021). Lisäksi huomattava osa laitevalmistajista ei tarjoa ohjelmistopäivityksiä tai tietoturvakorjauksia vahinkojen lieventämiseksi tai estämiseksi hyökkäyksen jälkeen (Silva-Trujillo et al., 2023).

Nykypäivän puettavat laitteet keräävät paljon tietoa, jota usein tallennetaan pilveen, hallitaan kolmansien osapuolien toimesta ja käytetään näyttämään käyttäjätietojen koontiversioita mobiililaitteilla (Fúster et al., 2022). Puettaviin laitteisiin tallennetut tiedot eivät aina ole salattuja. Laitteissa ei usein ole minkäänlaista salasanasuojausta, PIN-koodia tai biometrisiä turvatoimia, eikä tietojen käyttöön ole asianmukaista tunnistautumista. Jos laitteet joutuvat vääriin käsiin, on suuri riski, että arkaluonteisia tietoja voi vuotaa tai että käyttäjä voi joutua jopa henkeä uhkaavaan tilanteeseen. (Sorber et al., 2012.)

Etenkin useimmissa edullisissa laitteissa on enemmän turvallisuus- ja tietosuoja-aukkoja. Turvallisuuden näkökulmasta nämä edulliset laitteet eivät sisällä tarvittavia todennus- tai salausmenetelmiä, jotka varmistaisivat laitteiden itsensä tai niiden käsittelemien tietojen eheyden. Käyttäjien yksityisyys on vaarantunut, kozka ulkopuolisilla on mahdollisuus päästä käsiksi laitteiden käsittelemään arkaluonteiseen tietoon, sekä siksi, että kyseistä tietoa siirretään epävarmojen yhteyksien kautta pilvipalvelimille ja jaetaan kolmansien osapuolten yritysten kanssa. (Fúster et al., 2022.) Fúster et al. (2022) mukaan matalan tulotason ihmiset, jotka käyttävät edullisempia puettavan teknologian laitteita, saattavat olla alttiimpia turvallisuus- ja tietosuojaongelmille, erityisesti jos he eivät ole perehtyneet teknologiaan. Koska ihmisiä kuvataan usein kyberturvallisuuden heikoimpana lenkkinä, tulisi jokaisen puettavan laitteen

haavoittuvuuksien torjuntastrategia sisältää tietoa käyttäjille, siitä miten he voivat käyttää laitteitaan turvallisesti (Blow et al., 2020).

Puettavaa teknologiaa koskee useita lainsäädännöllisiä säädöksiä, kuten Health Insurance Portability and Accountability Act (HIPAA) ja yleinen tietosuoja-asetus (GDPR). Näiden säädösten mukaan arkaluonteiset tiedot on kerättävä, tallennettava ja siirrettävä turvallisesti. Kyberturvallisuuskäytäntöjen käyttöönotolla pyritään varmistamaan näiden lakien noudattaminen ja välttämään oikeudelliset seuraamukset. (Webb, 2022.) HIPAA kuitenkin koskee vain nimenomaan terveystietoja terveydenhuollon piirissä, eikä täten koske kaikkia puettavia laitteita, kuten älykelloja, jotka myös keräävät terveystietoa (Bouderheim 2023). GDPR-järjestelmässä läpinäkyvyyden periaate on läheisesti yhteydessä tiedon ja suostumuksen käsitteisiin. Tietojen antaminen/tiedotusilmoitus on olennainen vaatimus, jonka avulla käyttäjää voidaan informoida siitä, miten heidän tietojaan käsitellään. Tärkeimpiä asioita siinä ovat yhteystiedot, käyttötarkoitukset, laillinen peruste, tietojen säilytysaika ja siirto (tai siirron puuttuminen) ulkomaille, joihin lisätään myös tietojen vastaanottajat ja mahdollisuus käyttää omia oikeuksiaan. (Ziccardi, 2020.)

Konkreettisia kansallisia ja kansainvälisiä säädöksiä tulisi kehittää. Näiden säädösten tulisi käsitellä esimerkiksi laatuvaatimusten toteuttamista, terveystietoihin pääsyn ehtoja, yhteentoimivuutta sekä edustavuutta. Erityisen tärkeää on varmistaa keskeisten säädösten, kuten EU:n yleisen tietosuoja-asetuksen (GDPR) ja tulevan EU:n datasäädöksen, noudattaminen. EU:n datasäädöksen tavoitteena on yhdenmukaistaa sääntöjä, jotka koskevat oikeudenmukaista pääsyä dataan ja sen käyttöä julkisten ja yksityisten toimijoiden kesken. Kuten edeltäjänsä GDPR, EU:n datasäädös tulee auttamaan puettavien laitteiden käyttäjiä hallitsemaan terveystietojaan entistä tehokkaammin. Lisäksi se voi toimia ohjeistuksena tai mallina muille maille sekä vahvistaa keskeisiä kansainvälisiä standardeja terveystietojen yksityisyyden ja tietoturvan osalta. (Bouderhem 2023.)

Suurten riskien vuoksi puettavaa teknologiaa kehittävien yritysten tulisi toteuttaa asianmukaisia kyberturvatoimia. Standardoitua tarkistuslistaa ei ole, mutta toimenpiteet on mukautettava tilanteeseen (esimerkiksi kerätyn datan määrä ja luonne sekä mahdollisen tietomurron aiheuttamat kustannukset ihmisten oikeuksiin). Suojaus tulisi ehdottomasti sisällyttää jo tuotteen suunnitteluvaiheessa ja kehittämisessä ("yksityisyys suunnittelun lähtökohtana"), ja käyttäjällä tulisi olla täysi hallinta laitteeseensa. (Ziccardi, 2020.) Jotkut yritykset ovat viime aikoina keskittyneet myymään tuotteita, jotka takaavat käyttäjiensä yksityisyyden ja turvallisuuden. Kuitenkin suurilla verkkokauppapaikoilla tehdyn haun tulokset osoittavat, että merkittävä osa markkinoista koostuu

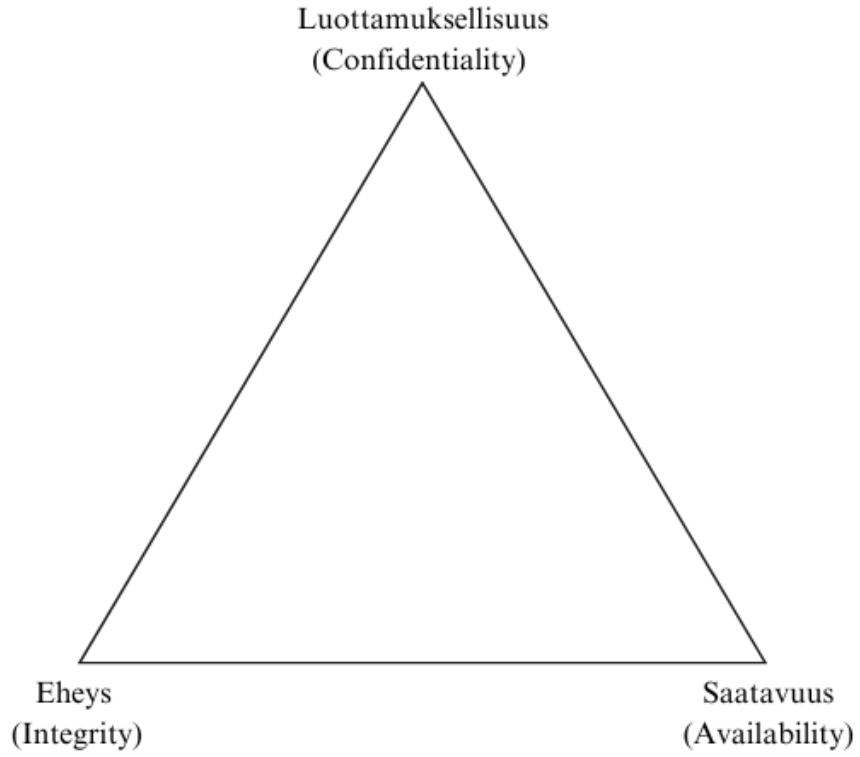
tuotteista, joilla ei ole tällaisia takeita. Nämä tuotteet ovat usein edullisia laitteita, jotka saavuttavat suuret myyntiluvut, mutta asettavat hinnan, käytettävyyden ja mukavuuden etusijalle turvallisuuden ja yksityisyyden kustannuksella. (Fùster et al., 2022.)

Markkinoiden kasvaessa nopeasti tarvitaan enemmän investointeja turvallisten puettavien teknologioiden tutkimukseen ja kehitykseen. Mikäli kyberturvallisuuden keskeisiä periaatteita ja käytäntöjä ei noudateta, tulevaisuus näyttää synkältä, kun hakkerit hyödyntävät riittämättömästi suojattuja tuotteita käyttäviä henkilöitä. (Andjelic et al., 2022.) Suoja kaikentyyppisiä kyberhyökkäyksiä vastaan on välttämätöntä tulevaisuuden teknologialle (Silva-Trujillo et al., 2023). Ilman sääntelyä hakkerit voivat tunkeutua vapaasti yksilöiden tai organisaatioiden yksityisyyteen, ja valmistajat voivat rikkoa käyttäjien oikeuksia huomaamattaan. Epäeettisen käytön riskiä voidaan vähentää asettamalla sitovia sääntöjä. (Andjelic et al., 2022.) Laitteiden valmistajilla ei ole selkeitä kannustimia sisällyttää turvallisuus- ja yksityisyysominaisuuksia, joten sääntely ja lainvalvonta ovat tarpeen sen varmistamiseksi, että laitteet täyttävät asianmukaiset turvallisuus- ja yksityisyysvaatimukset. (Fùster et al., 2023.) Tämä on erityisen tärkeää, kun tällaiset laitteet on suunnattu haavoittuville ryhmille, kuten alaikäisille (Schneider, 2017).

2.5 CIA kolmio

Jotta voidaan ymmärtää, kuinka vakavia nämä uhat ovat, puettavan teknologian käytön sekä arkaluonteisen tiedon keräämisen lisääntyessä on otettava huomioon haavoittuvuudet. Näitä haavoittuvuuksia voidaan mitata CIA-kolmion avulla), (ks Kuva 2). CIA-kolmio on yleisin tietoturvamalli, jota käytetään arvioimaan teknologian turvallisuusympäristöä. Se on keskeinen käsite kyberturvallisuudessa, jossa pyritään varmistamaan tietojärjestelmän luottamuksellisuus, eheys ja saatavuus (confidentiality, integrity ja availability). (Silva-Trujillo et al., 2023; Webb, 2022.) Luottamuksellisuus, eheys ja saatavuus (CIA) ovat vahvan ja kestävän verkon

suojausrakenteen perustavanlaatuisia periaatteita ja ne ovat liitoksissa turvallisten ohjelmistojen kanssa (Osazuva, 2023).



Kuva 2 CIA-kolmio, mukaillen Webb, (2022)

2.5.1 Luottamuksellisuus

Luottamuksellisuudella viitataan eettiseen ja oikeudelliseen velvoitteeseen suojata arkaluonteinen tieto luvattomalta pääsyltä tai paljastumiselta. Luottamuksellisuus liittyy suojatoimiin, jotka estävät luvattomia henkilöitä pääsemästä käsiksi arkaluonteisiin tietoihin. Tämä tarkoittaa, että arkaluonteisiin tietoihin tulisi päästä käsiksi vain virallisesti valtuutetut henkilöt tai organisaatiot. (Osazuva, 2023.) Puettavissa laitteissa esiintyy usein haavoittuvuuksia, koska tietoa siirretään älypuhelimiin ja pilvipalveluihin suojaamattomien Bluetoothin tai Wi-Fi yhteyksien avulla. Nämä yhteydet ovat suhteellisen helppoja murtaa. Mikäli tiedot joutuvat vääriin käsiin, voidaan niitä väärinkäyttää, jolloin luottamuksellisuus vaarantuu. (Mills et al, 2016.)

Puettavan teknologian uhat luottamuksellisuuden näkökulmasta liittyvät siihen, että käyttäjät eivät aina tiedosta laitteisiinsa sisältyviä tietoturvariskejä tai suojaa tietojaan riittävän hyvin. Monet käyttäjät eivät esimerkiksi ota käyttöön salattuja yhteyksiä tai monivaiheista tunnistautumista. (Mills et al., 2016.) Luottamuksellisuuden turvaamiseksi olisi kriittistä käyttää vahvoja

salausmenetelmiä datan siirrossa sekä tallennuksessa. On myös tärkeää varmistaa, että käyttäjät ovat koulutettuja ja tietoisia tietoturvasta. (Blow et al., 2020.)

2.5.2 Eheys

Eheys viittaa tiedon suojaamiseen luvattomilta muutoksilta tai vääristymiltä. Tämä edellyttää, että tietoja ei saa muuttaa ilman asianmukaista valtuutusta ja että kaikki muutokset on tallennettava ja dokumentoitava asianmukaisesti. (Osazuva, 2023.) Eheys voi vaarantua puettavissa laitteissa, mikäli tietoja päästään manipuloimaan. Tietoja voidaan manipuloida esimerkiksi hakkeroitumalla laitteeseen ja ohjelmoimalla se antamaan vääriä lukemia käyttäjän terveydentilasta. (Mills et al., 2016.) Vaikka eheys on oleellinen osa CIA kolmiota, tutkimustietoa koskien puettavien laitteiden eheyttä on rajallisesti (Webb, 2022).

2.5.3 Saatavuus

Saatavuus puolestaan tarkoittaa sitä, että valtuutetuilla henkilöillä on helppo pääsy tietoihin tarpeen mukaan. Tämä korostaa, kuinka tärkeää on suojata tietojärjestelmiä häiriöiltä, jotka voisivat estää käyttäjiä pääsemästä tietoihin. (Osazuva, 2023.) Taustapalvelimien ja verkkojen tulisi olla käyttäjien saatavilla ympäri vuorokauden, jotta valtuutettu käyttäjä voi käyttää tietojaan milloin tahansa (Webb, 2022). Älykellojen ainoa tunnettu saatavuuskatkos liittyi Garminiin kohdistuneeseen kiristysohjelmahyökkäykseen, joka pakotti yrityksen sulkemaan infrastruktuurinsa, mukaan lukien Garmin Connect -palvelun, joka sisältää käyttäjätietoja (Sweney, 2020).

Saatavuuden varmistamiseksi puettavissa laitteissa tarvitaan tehokkaita energianhallintaratkaisuja, kuten älykästä virransäästöä ja vaihtoehtoisia energialähteitä (Patel & Wang, 2019). Myös palvelunestohyökkäyksiltä (DoS) suojautuminen on tärkeää, sillä hyökkäykset voivat tehdä laitteen tai siihen liittyvät palvelut tilapäisesti käyttökelvottomiksi (Andjelic et al., 2022).

3 Miten nämä uhat voivat vaikuttaa käyttäjiin?

Puettavan teknologian kyberturvallisuusuhkien vaikutukset niiden käyttäjiin voivat olla vakavia ja moniuloitteisia. Ne eivät rajoitu vain digitaaliseen maailmaan vaan voivat vaikuttaa käyttäjien arkipäiväiseen elämään ja terveyteen monilla eri tavoilla. Terveydenhallintalaitteiden antamat virheelliset tiedot voivat aiheuttaa vakavia seurauksia käyttäjän hyvinvoinnille, ja laitteiden keräämän datan väärinkäyttö voi johtaa yksityisyydensuojaan liittyviin ongelmiin, kuten sijaintitietojen paljastumiseen tai arkaluonteisten tietojen joutumiseen vääriin käsiin. Lisäksi tietomurrot ja tietojen manipulointi voivat heikentää luottamusta teknologiaan, mikä saattaa hidastaa sen hyväksyntää ja laajempaa käyttöönottoa. On myös tärkeää huomioida, että palveluntarjoajat voivat laillisesti hyödyntää keräämäänsä dataa monenlaisiin tarkoituksiin, kuten esimerkiksi kohdennettuun mainontaan ja markkinointiin, tai myydä sitä eteenpäin kolmansille osapuolille. Tässä luvussa tarkastellaan puettavan teknologian tietoturvauhkien konkreettisia vaikutuksia käyttäjiin ja sitä, millaisia fyysisiä, psyykkisiä ja sosiaalisia seurauksia niillä voi olla.

3.1 Terveyshaitta

Puettavan teknologian laitteissa uhka ei kohdistu ainoastaan dataan vaan myös potentiaaliin aiheuttaa fyysistä haittaa. Haitat voivat vaihdella häiritsevästä jopa kuolettaviin seurauksiin. Johdannossa mainittiin, kuinka älykello voidaan esimerkiksi ohjelmoida lähettämään sarja häiritseviä, mutta merkityksettömiä pulsseja ilman mitään syytä. Diabeetikon käyttämä älypiilolinssi, joka seuraa verensokeripitoisuutta, voitaisiin myös hakkeroida niin, että se antaisi vääränlaisia tuloksia verensokerin tilasta. Tämänkaltaiset väärinkäytökset voivat johtaa vakaviin seurauksiin tai jopa henkilön kuolemaan. (Mills et al., 2016.) Silva-Trujillon et al. artikkelin (2023) mukaan tutkimukset ovat osoittaneet, että älykellon käyttäjät suhtautuvat vakavasti aktiivisuusilmoituksiin ja pitävät niitä terveydenhallinnan välineenä. Lisäksi on ilmennyt ilmiö, jossa käyttäjät kokevat stressiä tai ahdistusta älykellojen ja muiden digitaalisten hyvinvointityökalujen antamista terveyslukemista (Silva-Trujillo et al., 2023). Mikäli näitä tietoja manipuloidaan, käyttäjät voivat saada virheellistä tietoa terveydentilastaan, mikä saattaa johtaa turhaan huoleen tai aiheettomaan turvallisuuden tunteeseen. Tämä voi vaikuttaa heidän päätöksiinsä terveyden ylläpitämisestä ja johtaa jopa haitallisiin elämäntapamuutoksiin. Esimerkiksi laite voidaan ohjelmoida antamaan virheellistä tietoa verensokerista tai verenpaineesta. Tämä saattaa johtaa joko perusteettomaan turvallisuuden tunteeseen tai ylireagointiin johtuen virheellisestä mittaustuloksesta, esimerkiksi muuttamalla lääkityksen annostusta, vaikka todellisuudessa ei olisi mitään syytä huoleen. (Mills et al., 2016.)

3.2 Yksityisyys

Käyttäjät altistuvat monille turvallisuusuhille käyttäessään puettavia laitteita. Yleensä puettavan laitteen keräämät tiedot tallennetaan yhteen yrityksen tietokantaan, mikä voi altistaa kaikki käyttäjät tietosuojan vaarantuessa. (Els & Cilliers, 2017.) Murtautumalla laitteeseen voi kolmas osapuoli saada merkittävää tietoa käyttäjän käyttäytymisestä sekä liikkeistä ja käyttää sitä haitallisiin tarkoituksiin. (Mills et al., 2016). Yksityisyysongelmia syntyy, kun laaja joukko arkaluonteisia tietoja paljastetaan ilman käyttäjän tietoa tai suostumusta (Zhang et al., 2017).

Monet käyttäjät tiedostavat, että joitakin heidän tietojaan saatetaan käyttää palveluiden parantamiseen kolmansien osapuolten toimesta, mutta harvat ymmärtävät, minkä tyyppistä tai kuinka tarkkaa tämä data on. Esimerkiksi osa käyttäjistä saattaa sallia sijaintinsa keräämisen, mutta he eivät tiedä tarkasti, mitä tietoja heistä paljastetaan, kuten GPS-sijainti, kaupunki, kotiosoite ja useimmin vierailtuja paikkoja. Kun lääketieteellisten puettavien laitteiden käsittelemän datan määrä kasvaa, kasvaa myös riski arkaluonteisten tietojen paljastumisesta, joko datan siirron aikana pilveen tai tietojen säilyttämisen aikana laitteessa. (Sun et al. 2018.) Sijaintitiedot voivat paljastaa erittäin henkilökohtaisia yksityiskohtia henkilöstä, kuten sen, onko hän käynyt AIDS-klinikalla, lääkärin vastaanotolla tai uskonnollisissa paikoissa. Näitä tietoja voidaan väärinkäyttää ja käsitellä epäasianmukaisesti, erityisesti silloin, jos hakkerit saavat niihin pääsyn, tiedot myydään yrityksille, jotka voivat rakentaa käyttäjäprofiileja ilman kuluttajan suostumusta, tai ne kerätään seuraamissovellusten avulla. Paikkatiedot voivat myös helpottaa rikollista toimintaa, kuten vainoamista, perheväkivaltaa, murtoja ja kidnappauksia, koska niiden avulla voidaan helposti tunnistaa henkilön nykyinen tai tuleva sijainti. (Goh, 2015.) Äskettäin Pentagon myönsi, että kuntoseurantasovellus Strava© paljasti Yhdysvaltain sotilaiden sijainnit Syyrian ja Irakin sota-alueilla. Stravan kuntoseurantasovelluksen "lämpökartta"-ominaisuus pystyi paljastamaan Yhdysvaltain sotilastukikohtien sijainnit Syyriassa ja muilla konfliktialueilla sekä osan joukkojen liikkeistä. Lisäksi raportoitiin, että Strava mahdollisti käyttäjien tietojen de-anonymisoinnin, jolloin tallennettu käyttäjän nimi, nopeus ja jopa syke saattoivat paljastua. (Drape, 2018.)

Jotta yksityisyysongelmia voidaan ehkäistä, kehittäjien on myös lisättävä ohjeistuksia tuotteidensa käytöstä. Tämä hyödyttää sekä käyttäjiä että puettavien laitteiden kehittäjiä, sillä ohjeiden lisääminen auttaa suojaamaan asiakkaita, antamalla heille selkeän käsityksen laitteiden oikeasta käytöstä ja vähentää samalla mahdollisten oikeudellisten ongelmien riskiä tulevaisuudessa. (Alrababah, 2021; Moganedi & Pottas, 2020.)

3.3 Tietojen väärinkäyttö

Henkilötietoihin liittyvä data on digitaalinen, helposti jälleenmyytävä tuote. Puettavien laitteiden käyttäjät vaikuttavat hyväksyvän ajatuksen siitä, että heidän toimintaansa internetissä seurataan jatkuvasti. Mainostajille näin suurissa määrin kerätty data mahdollistaa oikean kohdeyleisön tavoittamisen oikeassa paikassa, oikeaan aikaan ja oikealla viestillä. Tämä tuo esiin huomattavia tietosuojariskejä. (Ioannidou & Sklavos, 2021.) Henkilökohtaisten tietojen arvo ei usein ole tiedossa, kun tietoa aletaan keräämään (eli silloin, kun ilmoitus ja suostumus tietojen keräämiseen yleensä annetaan). Lisäksi käyttäjien ja henkilötietoja käsittelevien tahojen välinen suhde on muuttunut yhä monimutkaisemmaksi, kun tietoa yhdistellään, siirretään, jaetaan tai myydään. (Banerjee et al., 2019.) Tällaiset henkilökohtaiset tiedot kuten käyttäjän syntymäaika ja sosiaaliturvatunnus ovat pimeillä markkinoilla usein monikertaisesti arvokkaampia kuin esimerkiksi varastettu luottokorttinumero (Overfelt, 2015).

Suostumusilmoitukset, jotka eivät paljasta kolmansien osapuolten henkilöllisyyksiä ja joilla on pääsy käyttäjän tietoihin, estävät kuluttajia tekemästä aidosti "tietoista" suostumuspäätöstä. Lisäksi nämä ilmoitukset ovat usein niin laajoja tai monimutkaisia, että käyttäjien on vaikea ymmärtää niitä, mikä heikentää tietoisen valinnan merkitystä. (Banerjee et al., 2019.) Mikäli puettavan laitteen keräämät tiedot päätyvät kolmannen osapuolen väärinkäytettäväksi, voidaan älylaitteen keräämiä tietoja käyttää tarkoitukseen, johon käyttäjä ei ole antanut lupaa. Laitteen käyttäjän käytöksestä voidaan myös oppia paljon ja tietoja voidaan käyttää esimerkiksi markkinointitarkoitukseen. Voidaan myös luoda vääriä tietoja käyttäjän terveydentilasta tai käytöksestä, mikä saattaa jopa johtaa väärien lääkkeiden määräämiseen. (Mills et al., 2016.)

Huolia herättää myös yritysten harjoittama käyttäjäprofiilien luonti (profilointi) kuluttajien tarpeiden kartoittamiseksi ja mainosmarkkinoinnin mukauttamiseksi näiden mieltymysten mukaan. Useimmissa tapauksissa tämä toteutetaan tallentamalla ja keräämällä systemaattisesti tietoa käyttäjistä. Näin palvelut ja sovellukset saattavat olla ilmaisia, mutta tosiasiassa käyttäjien toiminnasta kerätyt tiedot muodostuvat todelliseksi valuutaksi, joka usein myydään myöhemmin kolmansille osapuolille. Vaikka mainonnan strategiat eivät välttämättä aiheuta suoraa haittaa käyttäjälle, heidän identiteettinsä rakentaminen ja paljastaminen tai pääsy laitteiden tiettyihin toimintoihin (kuten puhelut, SMS-viestien luku, GPS-seuranta, tallennus) ja sisältöön (kuten valokuvat, videot, yhteystiedot, viestit) ilman ennakkoilmoitusta tai lupaa, katsotaan selkeäksi yksityisyyden loukkaukseksi. (Ioannidou & Sklavos, 2021.) Yritykset voivat kerätä ja kaupata puhelimien ja puettavien laitteiden antamia tietoja selvittääkseen käyttäjän mielialaa, stressitasoa,

tapoja, hyvinvointia, unikäyttäytymistä, liikuntaa ja liikkeitä. Koska datan määrä puettavissa laitteissa on usein niin suuri, voidaan siitä luoda kattavia analyysejä. Näitä tietoja käyttäjän tavoista ja tottumuksista voidaan käyttää hyväksi esimerkiksi luottopäätöksissä, vakuutuksissa ja työllistymispäätöksissä, mikä voi vaarantaa yksityisyyden ja jopa aiheuttaa esteitä terveydenhuollon saamiselle. (Banerjee et al., 2018; Ziccardi, 2020.) Tietosuojaloukkausten mahdollisia haitallisia seurauksia voivat myös olla syrjivä profilointi, manipuloiva markkinointi ja tietomurrot (Montgomery et al., 2018).

Vastaavana esimerkkinä tietojen väärinkäytöstä ja sen seurauksista voidaan tarkastella psykoterapiakeskus Vastaamon tapausta vuodelta 2020. Siinä hyökkääjä sai haltuunsa tuhansien potilaiden arkaluonteisia tietoja ja käytti niitä kiristystarkoituksiin (Heikkilä & Cerulus, 2020). Pian hyökkäyksen jälkeen useat kyberturvallisuusyritysten raportit osoittivat, että tietovuoto ei ollut seurausta kehittyneestä hyökkäyksestä, vaan johtui Vastaamon puutteellisesta tietoturvakäytännöstä (Ghanbari & Koskinen, 2024). Helsingin Sanomien artikkelin (2024) mukaan ihmisiä on päätynyt jopa itsemurhaan tietojen vuotamisen takia. Tapaus korostaa, kuinka vakavia seurauksia yksityisten tietojen paljastumisella voi olla käyttäjien psyykkiselle ja sosiaaliselle hyvinvoinnille.

4 Esimerkkicase Fitbit

Tutkielman kannalta on mielekästä tutkia yritystä, jolla on esiintynyt tietoturvaongelmia menneisyydessä. Esimerkiksi valikoitui siis kansainvälisesti merkittävä älykellojen ja aktiivisuusrannekkeiden valmistaja Fitbit. Vuonna 2023 Fitbit-laitteita myytiin maailmanlaajuisesti yli 6,6 miljoonaa kappaletta (D'Souza, 2024.) Analysoimalla Fitbitiin liittyviä haavoittuvuuksia ja tietoturvaongelmia, tapaustutkimus tarjoaa arvokkaita näkökulmia siihen, millaisia seurauksia riittämättömillä tietosuojatoimilla voi olla. Lisäksi Fitbitin erityisten haasteiden tarkastelu auttaa tunnistamaan laajempia kaavoja ja oppeja, joita voidaan soveltaa koko puettavan teknologian alalla. Luvussa käsitellään Fitbit-laitteiden haavoittuvuuksia ja sitä miten ne johtivat vuonna 2021 tietovuotoon. Lisäksi luvussa pohditaan, miten tämänkaltaisia tietovuotoja voitaisiin välttää.

Fitbit-laitteista on löytynyt haavoittuvuus, Fitbit-laitteen ja pilvipalvelimen välillä vaihdettu data voidaan siepata. Tämän seurauksena hyökkääjät saattavat saada pääsyn Fitbit-käyttäjien arkaluonteisiin tietoihin ja luoda väärennettyjä aktiivisuustietoja, joita he voivat siirtää kolmansille osapuolille, joilla ei ole lupaa nähdä näitä tietoja. (Andjelic et al. 2022.) Fitbit on suunniteltu kuluttajien aktivoimiseksi ja liikkeessä pitämiseksi, laitteesta puuttuu kuitenkin tietoturvaominaisuuksia, jonka vuoksi käyttäjät ja heidän organisaationsa altistuvat mahdollisille hyökkäyksille. Tämä tietoturvan puute voi houkutella hakkereita ja rikollisia kohdistamaan toimiaan tähän laitteeseen hyödyntääkseen työntekijöiden ja yrityksen tietoja. (Blow et al., 2020.) Rahmanin et al. (2013) tutkimus tutki Fitbit One -laitteen tietoturvan tilaa, ja tutkimuksen tulokset osoittivat, että kaikki tiedonsiirto tukiaseman ja myyjän verkkosivuston välillä oli salaamatonta. Näin ollen puettavan laitteen valmistajan tai palveluntarjoajan pilvipalvelimelle tallennetut tiedot ovat erittäin haavoittuvia, koska palveluntarjoajat eivät olleet käyttäneet salausta (Carlson, 2017).

Fierce healthcare lehdessä julkaistussa artikkelissa (Landi, 2021) kerrotaan, kuinka kesäkuussa 2021 paljastui suojaamaton tietokanta, joka sisälsi yli 61 miljoonaa tietuetta muun muassa Fitbitin kaltaisista aktiivisuusmittareista, paljastaen arkaluonteisia käyttäjätietoja, kuten nimiä, syntymäaikoja, painoja, pituuksia, sukupuolia ja sijaintitietoja. Vaikka tietomurto ei alun perin ollut peräisin suoraan Fitbitin järjestelmistä, tapaus korostaa merkittäviä yksityisyysriskejä, jotka liittyvät kolmansien osapuolien integraatioihin ja pilvipohjaisien tietojen tallennuksen haavoittuvuuksiin.

Blow et al. ovat tutkimuksessaan (2020) todenneet, että yksi tapa estää Fitbitin tietosuojaongelmat olisi siirtyä BLE-teknologiasta lähikenttäviestintään (NFC). NFC:n toimintaetäisyys on vain noin 4 senttimetriä, kun taas Bluetooth tukee yhteyksiä jopa yli 9 metrin päästä. Koska useimmat Fitbit-

laitteet käyttävät Bluetooth-yhteyttä, niiden pariliitostoiminnot altistavat ne suuremmalle määrälle mahdollisia kyberuhkia, kuten Man-in-the-Middle hyökkäyksille ja porttiskannausten kaltaisille hyökkäyksille, jotka hyödyntävät pitempää viestintäetäisyyttä. Myös Silva-Trujillo et al. (2023) on todennut, että laitteiden välisten yhteyksien, kuten BLE-yhteyksien turvaamisen tulisi olla seuraava askel puettavien laitteiden tietoturvan takaamisessa.

5 Pohdinta ja johtopäätökset

Tässä tutkielmassa tutkittiin puettavan teknologian kyberturvallisuuteen ja tietosuojaan liittyviä uhkia. Tutkielmassa tarkastellaan erityisesti puettavan teknologian laitteita, jotka keräävät terveyteen liittyviä tietoja, kuten älykelloja ja aktiivisuusmittareita. Lisäksi puettavaa teknologiaa käsitellään myös yleisemmällä tasolla.

Ensimmäinen tutkimuskysymys käsitteli puettavaan teknologiaan liittyviä uhkia. Puettavaan teknologiaan kohdistuu monenlaisia kyberturvallisuusuhkia, kuten tietomurrot, tietojen väärinkäyttö, epäluotettavat sovellukset sekä kyberhyökkäykset. Nämä uhat ilmenevät esimerkiksi tietojen salakuunteluna, tietoliikenteen analysointina ja tietovuotoina, joissa hyökkääjä voi kerätä, manipuloida tai paljastaa arkaluonteisia käyttäjätietoja. Tämä voi vaarantaa käyttäjän yksityisyyden ja pahimmillaan jopa fyysisen turvallisuuden, mikäli tietomurto kohdistuu terveystietoihin tai sijaintitietoihin. Tietoturvariskit liittyvät myös laitteiden suojaamattomiin yhteyksiin, kuten Bluetooth-yhteyksiin, ja pilvipalveluihin, joihin tietoja tallennetaan.

Toisen tutkimuskysymyksen avulla pyrittiin selvittämään, miten uhat vaikuttavat käytännössä käyttäjiin. Käyttäjiin kohdistuvat vaikutukset voivat olla vakavia ja monimuotoisia. Fyysiset haitat voivat vaihdella lievistä häiriöistä hengenvaarallisiin tilanteisiin, kuten diabeetikon älylaitteen antaessa vääriä glukoosilukemia. Yksityisyyden loukkaukset voivat paljastaa käyttäjän henkilökohtaisia terveystietoja, sijaintia tai muita arkaluonteisia tietoja. Lisäksi tiedon väärinkäytöstä voi seurata vakavia taloudellisia ja maineeseen liittyviä seurauksia, kun tietoja jaetaan luvatta kolmansille osapuolille.

Akateemista kirjallisuutta analysoidessa nousi useasti esiin puettavan teknologian tietosuojan tämänhetkinen heikkous. Lainsäädäntöä on kehitettävä ja yritysten on parannettava laitteiden tietoturvaa, sillä tietoturvan puute luo useita riskejä käyttäjille. Toisaalta myös puettavan teknologian laitteiden käyttäjillä on velvollisuus olla tietoisia laitteidensa tietoturva-asetuksista ja pyrkiä suojautumaan mahdollisilta hyökkäyksiltä. Kuitenkin lisää koulutusta ja tietoisuuden lisäämistä tarvitaan puettavan teknologian jatkuvasti lisääntyessä, jotta käyttäjät voivat toimia turvallisesti. Kirjallisuuden rajoitteena oli teknologian nopea kehittyminen, mikä rajoitti akateemisen kirjallisuuden saatavuutta. Lisäksi aihetta käsiteltiin usein samasta näkökulmasta. Tämän seurauksena yleistettävyys voi olla osittain rajallinen, sillä osa kirjallisuudesta keskittyy vain tiettyihin puettavan teknologian laitteisiin, eikä välttämättä kata kaikkia laitekategorioita. Lisäksi osa käytetyistä lähteistä saattaa olla vanhentuneita nopeasti kehittyvän teknologian ja laajentuvien

markkinoiden vuoksi, mikä voi vaikuttaa niiden todenperäisyyteen ja soveltuvuuteen nykytilanteessa.

Tulevaisuudessa olisikin tärkeää tutkia, millä tavoin puettavien laitteiden tietoturvaa voidaan parantaa esimerkiksi käyttämällä hyödyksi uusinta teknologiaa. Lisäksi puettavaan teknologiaan liittyvän lainsäädännön ja säädösten vaikutuksia tulisi analysoida syvemmin. Puettava teknologia kehittyy vauhdilla, jonka takia lainsäädäntö ei ole pysynyt kehityksen mukana. Siksi olisikin tarkasteltava lainsäädäntöä ja säädöksiä pitemmällä tähtäimellä ja pyrkiä ennakoimaan mahdollisia riskejä, jotta niihin voitaisiin varautua hyvissä ajoin.

Tietosuojan ja kyberturvallisuuden turvaaminen on keskeinen osa puettavan teknologian kehitystä. Puettavaan teknologiaan kohdistuu merkittäviä kyberturvallisuus- ja tietosuojauhkia, kuten tietojen väärinkäyttöä, tietomurtoja ja yksityisyyden loukkauksia. Näiden uhkien seuraukset voivat olla vakavia, ulottuen jopa käyttäjien fyysiseen turvallisuuteen ja yksityisyydensuojaan.

Tutkielmassa havaittiin erilaisia käytännön seurauksia eri puettavaan teknologiaan liittyville sidosryhmille. Laitteiden kehittäjien ja valmistajien on kiinnitettävä erityistä huomiota tietoturvaan jo suunnitteluvaiheessa. Esimerkiksi laitteisiin tulisi asentaa vahvempia salausmenetelmiä ja pohtia, onko esimerkiksi tiedonsiirrolle turvallisempia vaihtoehtoja kuin nykyisin yleisimmät Wi-Fi ja BLE-yhteydet. Ohjelmistopäivitykset tulisi myös varmistaa niin, että laitteiden tietoturva pysyy varmasti ajan tasalla.

Loppukäyttäjien tietoisuuden lisääminen tietoturvasta on erityisen tärkeää. Käyttäjien tulee olla tietoisia, miten laitteiden tietoturva-asetuksia käytetään ja miksi ne ovat tärkeitä. Käyttäjien tulee myös olla tietoisia siitä, miten pitää kyberturvallisuus ja tietosuoja mahdollisimman hyvänä. Olisi myös tärkeää, että käyttäjät ovat tietoisia siitä, mitä tietoja laitteet oikeastaan keräävät ja mihin niitä voidaan käyttää.

Lainsäädännön ja säädösten merkitys puettavien laitteiden kyberturvallisuuden varmistamisessa ja tietosuojauhkien eliminoimisessa korostuu puettavan teknologian kehittyessä. On tärkeää ennakoida kehitystä ja luoda säädöksiä, jotka tukevat laitteiden turvallista käyttöä. Yrityksille on myös asetettava tietoturvastandardeja, jotka laitteiden pitää täyttää.

Lähteet

Acharya, A., & Raje, R. R. (2000). MAPbox: Using parameterized behavior classes to confine applications. Proceedings of the 9th USENIX Security Symposium, 1–17. Retrieved from https://www.usenix.org/legacy/events/sec2000/full_papers/acharya/acharya.pdf

Alrababah, Z. (2020). Privacy and security of wearable devices. International Journal of Innovative Science and Research Technology, 5(12), 1–5.

Andjelic, S., Doyle, C., & Hossain, G. (2022). Cybersecurity risk with wearable technology in sports: Why should we care? HONET 2022: 19th International Conference on Smart Communities, Communication Networks and Technologies. https://doi.org/10.1109/HONET56683.2022.10019146

Arias, O., Wurm, J., Hoang, K., & Jin, Y. (2015). Privacy and security in internet of things and wearable devices. IEEE Transactions on Multi-Scale Computing Systems, 1(2), 99-109. https://doi.org/10.1109/TMSCS.2015.2498605

Banerjee, S., Hemphill, T., & Longstreet, P. (2018). Wearable devices and healthcare: Data sharing and privacy. *The Information Society*, *34*(1), 49–57. https://doi.org/10.1080/01972243.2017.1391912

Blow, F., Hu, Y.-H., & Hoppa, M. A. (2020). A study on vulnerabilities and threats to wearable devices. Journal of The Colloquium for Information Systems Security Education, 7(1), 34–45.

Bouderhem, R. (2023). Privacy and regulatory issues in wearable health technology. Proceedings of the 10th International Electronic Conference on Sensors and Applications, 58(1), 87. https://doi.org/10.3390/ecsa-10-16206

Canali, S., Schiaffonati, V., & Aliverti, A. (2022). Challenges and recommendations for wearable devices in digital health: Data quality, interoperability, health equity, fairness. PLOS Digital Health, 1(10), e0000104. https://doi.org/10.1371/journal.pdig.0000104

Carlson, H. (2017). Potential security threats to wearable technology. Retrieved from https://axiomcyber.com/cybersecurity/potential-security-threats-to-wearable-technology/. Vierailtu 8.11.2024

Chang, V., Xu, X., Wong, B., & Mendez, V. (2019). Ethical problems of smart wearable devices. In Proceedings of the 4th International Conference on Complexity, Future Information Systems and Risk (pp. 1–8).

Cheng, L., Liu, F., & Yao, D. D. (2017). Enterprise data breach: Causes, challenges, prevention, and future directions. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 7(5), e1211. https://doi.org/10.1002/widm.1211

D'Souza, J. (2024, November 6). Fitbit statistics by revenue, sales and usage. Coolest Gadgets. Retrieved from https://www.coolest-gadgets.com/fitbit-statistics/

Drape, S. (2018). How data breach is inevitable in wearable devices. Wearable Technologies. https://www.wearable-technologies.com/2018/08/pentagon-tells-soldiers-to-leave-wearable-trackers-at-home-when-heading-to-warzones/

Els, F., & Cilliers, L. (2017). Improving the information security of personal electronic health records to protect a patient's health information. In Proceedings of Information Communication Technology and Society Conference, Umhlanga, South Africa, 9–10 March 2017.

Erkkilä, J. (2021, 20.5.). Älykellojen myynti lähes tuplaantui – taustalla oman kehon mittaamisen trendi. SalkunRakentaja. https://www.salkunrakentaja.fi/2021/05/alykellot-myynti-kehon-mittaaminen/

Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2012). Android permissions: User attention, comprehension, and behavior. In Proceedings of the Eighth Symposium on Usable Privacy and Security (pp. 3:1–3:14). https://doi.org/10.1145/2335356.2335360

Fúster, J., Solera-Cotanilla, S., Pérez, J., Vega-Barbas, M., Palacios, R., Álvarez-Campana, M., & Lopez, G. (2022). Optimization of power control and resource allocation in cloud-based wireless wearable networks. Wireless Networks, 28(1), 75-90. https://doi.org/10.1007/s11276-022-03211-6

Ghanbari, H., & Koskinen, K. (2024). When data breach hits a psychotherapy clinic: The Vastaamo case. Journal of Information Technology Teaching Cases, 0(0). https://doi.org/10.1177/20438869241258235

Goh, Janice Phaik Lin. (2015). Privacy, security, and wearable technology. Landslide, 8(2), 30-58.

Grand View Research. (2022). Smartwatch market size, share & trends analysis report by product (extension, standalone), by application (personal assistance, wellness, healthcare, sports), by region, and segment forecasts, 2022 - 2030. Grand View Research. https://www.grandviewresearch.com/industry-analysis/smartwatch-market

Heikkilä, M., & Cerulus, L. (2020, October 26). Hacker seeks to extort Finnish mental health patients after data breach. Politico.

Helsingin Sanomat. (2024, December 15). *Vastaamo-uhrien juristi: Ihmisiä on päätynyt itsemurhaan tietomurron ja kiristyksen takia,* Retrieved from https://www.hs.fi/suomi/art-2000010265660.html

Ioannidou, I., & Sklavos, N. (2021). On General Data Protection Regulation vulnerabilities and privacy issues for wearable devices and fitness tracking applications. Cryptography, 5(4), 29. https://doi.org/10.3390/cryptography5040029

Jain, A. K., & Shanbhag, D. (2012). Addressing security and privacy risks in mobile applications. IT Professional, 14(5), 28–33. https://doi.org/10.1109/MITP.2012.72

Kantarcioglu, M., & Clifton, C. (2005). Security issues in querying encrypted data. In S. Jajodia & D. Wijesekera (Eds.), Data and Applications Security XIX (pp. 325–337). Springer. https://doi.org/10.1007/11535706_24

Kapoor, V., Singh, R., Reddy, R., & Churi, P. (2020). Privacy issues in wearable technology: An intrinsic review. Proceedings of the International Conference on Innovative Computing & Communications (ICICC) 2020. https://doi.org/10.2139/ssrn.3566918

Katurura, M., & Cilliers, L. (2017). A review of the implementation of electronic health record systems on the African continent. In Conference Proceedings of African Computer and Information System & Technology 2017, Cape Town, South Africa, 10–11 July 2017.

Kim, S. H., Wang, Q.-H., & Ullrich, J. B. (2012). A comparative study of cyberattacks. Communications of the ACM, 55(3), 66–73. https://doi.org/10.1145/2093548.2093568

Kolias, C., Stavrou, A., Voas, J., Bojanova, I., & Kuhn, R. (2016). Learning Internet-of-Things security "hands-on". IEEE Security & Privacy, 14(1), 37–46. https://doi.org/10.1109/MSP.2016.4

Kshetri, N. (2013). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommunications Policy, 37(4-5), 372-386. https://doi.org/10.1016/j.telpol.2012.04.011

Kyytsönen, M., Vehko, T., Anttila, H., & Ikonen, J. (2023). Factors associated with use of wearable technology to support activity, well-being, or a healthy lifestyle in the adult population and among older adults. PLOS Digit Health, 2(5), e0000245. https://doi.org/10.1371/journal.pdig.0000245

Landi, H. (2021, September 13). Fitbit, Apple user data exposed in breach impacting 61M fitness tracker records. Fierce Healthcare. https://www.fiercehealthcare.com/digital-health/fitbit-apple-user-data-exposed-breach-impacting-61m-fitness-tracker-records

Mills, A. J., Watson, R. T., Pitt, L., & Kietzmann, J. (2016). Wearing safe: Physical and informational security in the age of the wearable device. Business Horizons, 59(6), 615–622. https://doi.org/10.1016/j.bushor.2016.08.003

Moganedi, S., & Pottas, D. (2020). Threats and vulnerabilities affecting fitness wearables: Security and privacy theoretical analysis. In M. Loock, M. Coetzee, & J. Eloff (Eds.), Information and Cyber Security (pp. 57–68). Springer. https://doi.org/10.1007/978-3-030-43276-8_5

Montgomery, K., Chester, J., & Kopp, K. (2018). Health wearables: Ensuring fairness, preventing discrimination, and promoting equity in an emerging Internet-of-Things environment. Journal of Information Policy, 8, 34–77.

Motti, V. G., & Caine, K. (2015, January). Users' privacy concerns about wearables. In International Conference on Financial Cryptography and Data Security (pp. 231-244). Springer, Berlin, Heidelberg.

Ometov, A., Bezzateev, S., Kannisto, J., Harju, J., Andreev, S., & Koucheryavy, Y. (2017). Facilitating the Delegation of Use for Private Devices in the Era of the Internet of Wearable Things. IEEE Internet of Things Journal, 4(4), 843-854. https://doi.org/10.1109/JIOT.2016.2593898

Ometov, A., Shubina, V., Klus, L., Skibińska, J., Saafi, S., Pascacio, P., ... & Lohan, E. S. (2021). A survey on wearable technology: History, state-of-the-art and current challenges. Computer Networks, 193, 108074. https://doi.org/10.1016/j.comnet.2021.108074

Olabenjo, B., & Makaroff, D. (2019). Information leakage in wearable applications. https://doi.org/10.1007/978-3-030-24907-6_17

Osazuwa, O. M. C. (2023). Confidentiality, integrity, and availability in network systems: A review of related literature. International Journal of Innovative Science and Research Technology, 8(12)

Overfelt, M. (2015, December 13). The price of the wearable craze: Less data security. NBC News. http://www.nbcnews.com/tech/innovation/price-wearable-craze-less-data-security-n479271

Patel, M., & Wang, J. (2019). Energy harvesting for wearable devices: A review. IEEE Sensors Journal, 19(20), 8371–8384. https://doi.org/10.1109/JSEN.2019.2929971

Perera, C., Liu, C. H., & Jayawardena, S. (2015). The emerging internet of things marketplace from an industrial perspective: A survey. IEEE Transactions on Emerging Topics in Computing, 3(4), 585–598. https://doi.org/10.1109/TETC.2015.2390034

Piwek, L., Ellis, D. A., Andrews, S., & Joinson, A. (2016). The rise of consumer health wearables: Promises and barriers. PLOS Medicine, 13(2), e1001953. https://doi.org/10.1371/journal.pmed.1001953

Quinn, B. (2013). Technology and future fashion: Body technology for the twenty-first century. In S. Black, A. de la Haye, J. Entwistle, A. Rocamora, R. A. Root, & H. Thomas (Eds.), *The handbook of fashion studies* (pp. 436–455). Bloomsbury.

Rahman, M., Carbunar, B., & Banik, M. (2013). Fit and vulnerable: Attacks and defenses for a health monitoring device. In 34th IEEE Symposium on Security and Privacy.

Ramezanpour, B., Taneja, P., Bennis, M., & Hamalainen, T. (2021). Coexistence of 5G and Wi-Fi networks: A comprehensive survey. IEEE Communications Surveys & Tutorials, 23(4), 2068–2109. https://doi.org/10.1109/COMST.2021.3108111

Rauti, S., & Laato, S. (2020). Location-based games as interfaces for collecting user data. In Á. Rocha, H. Adeli, L. P. Reis, S. Costanzo, I. Orovic, & F. Moreira (Eds.), Trends and Innovations in Information Systems and Technologies (Vol. 1160, pp. 631–642). Springer. https://doi.org/10.1007/978-3-030-45691-7_59

Riek, M., & Böhme, R. (2018). The economics of data breach notifications. Journal of Cybersecurity, 4(1), tyy023. https://doi.org/10.1093/cybsec/tyy023

Satria, D., Sahid, S., Sujarwo, Sunardi, S., & Manurung, R. (2022). Development of online learning media for PLC programming in vocational education. International Journal of Online and Biomedical Engineering (iJOE), 18(9), 108-121. https://doi.org/10.3991/ijoe.v18i09.32255

Schneier, B. (2017). Regulating the internet of things. RSA Conference. https://www.youtube.com/watch?v=b05ksqy9F7k

Shabtai, A., Bercovitch, M., Rokach, L., & Elovici, Y. (2014). Optimizing data misuse detection. ACM Transactions on Knowledge Discovery from Data, 8(3), Article 16, 1–23. https://doi.org/10.1145/2611520

Siboni, S., Shabtai, A., Tippenhauer, N. O., Lee, J., & Elovici, Y. (2016). Advanced security testbed framework for wearable IoT devices. ACM Transactions on Internet Technology, 16(4), Article 26. https://doi.org/10.1145/2981546

Silva-Trujillo, A. G., González González, M. J., Rocha Pérez, L. P., & García Villalba, L. J. (2023). Cybersecurity analysis of wearable devices: Smartwatches passive attack. Sensors, 23(12), 5438. https://doi.org/10.3390/s23125438

Solove, D. J. (2006). A taxonomy of privacy. University of Pennsylvania Law Review, 154(3), 477-560. https://doi.org/10.2307/40041279

Sorber, J., Shin, M., Peterson, R., Cornelius, C., Mare, S., Prasad, A., Marois, Z., Smithayer, E., & Kotz, D. (2012). An amulet for trustworthy wearable mHealth. In Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications (pp. 7:1–7:6). ACM. https://doi.org/10.1145/2162081.2162092

Sun, W., Cai, Z., Li, Y., Liu, F., Fang, S., & Wang, G. (2018). Security and privacy in the medical internet of things: A review. Security and Communication Networks, 2018, 1–9. https://doi.org/10.1155/2018/5978636

Webb, A. J. (2022). Cyber security of smart watches: A review of the vulnerabilities with recommendations presented to protect the wearables. International Journal of Network Security & Its Applications (IJNSA), 14(3), 39–56. https://doi.org/10.5121/ijnsa.2022.14304

Wolf, B. C., Polonetsky, J., & Finch, K. (2016). A practical privacy paradigm for wearables. Washington, DC: Future of Privacy Forum.

Ziccardi, G. (2020). Wearable technologies and smart clothes in the fashion business: Some issues concerning cybersecurity and data protection. Laws, 9(2), 12. https://doi.org/10.3390/laws9020012

Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., & Shen, X. S. (2017). Security and privacy in smart city applications: Challenges and solutions. IEEE Communications Magazine, 55(1), 122–129. https://doi.org/10.1109/MCOM.2017.1600267CM

Chauhan, J., Seneviratne, S., Kaafar, M. A., Mahanti, A., & Seneviratne, A. (2016). Characterization of early smartwatch apps. In Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (pp. 1–6). Sydney, Australia.