

Tehtävä 1: Esineiden internet

Esineiden internet (Internet of Things, IoT) tarkoittaa verkkoon yhteydessä olevia laitteita ja esineitä, jotka pystyvät olemaan vuorovaikutuksessa oman ympäristönsä kanssa. Näiden laitteiden tarkoitus on muun muassa helpottaa ihmisten arkea ja tehostaa teollisuuden prosesseja.

IoT-laitteet voidaan jaotella kolmeen kategoriaan sen mukaan, millaisia vuorovaikutus- ja ohjausmahdollisuuksia laitteet sisältävät. Ensimmäinen kategoria on älykkäät esineet, jotka kykenevät kommunikoimaan internetverkon välityksellä joko toisen älykkään esineen tai verkossa toimivien tietojärjestelmien (muun muassa niin kutsuttujen pilvipalveluiden) kanssa. Tällaisia esineitä löytyy yhä enemmän myös tavallisten ihmisten kodeista. Tyypillisiä verkotettuja esineitä ovat älykellot, älytelevisiot, internetin kautta ohjattavat valot tai vaikkapa reaaliajassa sähkönkulutustietoja välittävät pistorasiat. Yksi esimerkki siitä, millaisia mahdollisuuksia älykkäät esineet tuovat koteihin, on järjestelmä, jonka kautta mikrofoni välittää ääntä kotoa älypuhelimeen. Tällöin isäntä kuulee, kun koira alkaa haukkua kotona. Isäntä voi sitten kännykäsovelluksen avulla antaa koiralle ruokaa tai juotavaa etäohjatusti.

Toinen IoT-laitteiden kategoria on laitteet, jotka keräävät sensoreiden avulla dataa ympäristöstään, kuten jonkin koneen tilasta ja sen käyttöolosuhteista. Tällaiset laitteet eivät välttämättä ole kytkettynä internetiin, mutta niiden keräämä data voidaan lukea aika ajoin vaikkapa datakaapelin välityksellä. Lisäksi tähän kategoriaan voidaan lukea niin kutsutut toimilaitteet (engl. actuator), kuten tietyt sähkömoottorit ja -magneetit. Toimilaitteilla voidaan vaikuttaa automaatiolla ohjattavaan prosessiin. Eräs tämän kategorian IoT-laite on moderni auto. Erilaiset sensorit, kuten kamerat, etäisyysensorit ja lämpömittarit, keräävät reaaliajassa tietoa ympäristöstään. Vastaavasti kaasun, jarrun ja virtalukon muodostavat muiden ohjausjärjestelmien kanssa yhden IoT-laitteiden verkon. Nämä ohjausjärjestelmät eivät kuitenkaan tyypillisesti kommunikoi julkiseen internetiin mitään, vaan tähän verkkoon päästään tarvittaessa käsiksi huoltoliikkeessä erityisen kaapelin välityksellä. Tosin nykyautoissa on usein myös erillinen viihde- ja navigointiverkko, joka koostuu älykkäistä internetiin kytketyistä (ensimmäisen kategorian) IoT-laitteista.

Kolmannen kategorian esineet ovat osa tietojärjestelmää, mutta eivät välttämättä ole erityisen älykkäitä, eivätkä ole aktiivisesti osa verkkoa. Tällaisia esineitä ovat esimerkiksi sirukortit, kuten etäluettavat bussikortit, joista voidaan lukea tai joille voidaan kirjoittaa tietoa langattomasti.

Esineiden internet ymmärretään tässä aineistossa siis laajasti kaikkien edellä mainittujen kolmen kategorian yhdisteeksi, erilaisia teknologioita ja käyttötarkoituksia käsittäväksi kokonaisuudeksi.

IoT-laitteet voidaan myös ryhmitellä sen mukaan, lähettävätkö tai vastaan-

ottavatko ne tietoa. Viestintä voi olla yksisuuntaista tai kaksisuuntaista. Yksisuuntaista viestintää toteuttavassa laitteessa *joko* laite lähettää *tai* laitteelle voi lähettää viestejä. Esimerkiksi yksinkertainen etäluettava lämpömittari lähettää tietoa lämpötilasta, mutta lämpömittarille ei voida lähettää viestejä. Kaksisuuntaista viestintää hyödyntävä IoT-laite voi sekä lähettää että vastaanottaa viestejä. Edellistä esimerkkiä mukaillen käyttäjä voisi esimerkiksi pienentää lämmitystä huomattavasti lämpötilan olevan korkealla.

Teollisuudessa IoT ja sen avulla kerätty data voivat auttaa yrityksiä tekemään päätöksiä, säästämään kustannuksia tai ennaltaehkäisemään vahinko- tai vaaratilanteita. Verkottuneita IoT-laitteita voivat olla paperikoneen rullat, hitsauslaitteet, tuulivoimalan turbiinit tai sataman kontinkuljetusjärjestelmään verkotetut laitteet. Esimerkiksi hitsauslaitteita ja -ohjelmistoja tarjoava yritys voi kytkeä hitsauslaitteet verkossa toimivaan palveluun, jonne välittyy kaikki tieto hitsaustapahtumasta, kuten kohteen hitsaaja, työssä käytetyt asetukset ja lisäaineet. Ennen työtehtävää henkilö skannaa henkilökorttinsa viivakoodin, minkä jälkeen hitsaustapahtumasta syntyvä data tallennetaan yrityksen päätöksenteon ja laadunvalvonnan tueksi. Toisaalta IoT voi helpottaa rutiininomaisia tehtäviä. Esimerkiksi ennen kiinteistöhoitaja kävi lukitsemassa rakennuksen ulko-ovet tiettyyn kellonaikaan, mutta nykyään lukitseminen voidaan ajoittaa tarkasti etänä, internetin välityksellä.

Eräitä kasvavia arkisia IoT-tuotteiden ryhmiä ovat lelut ja lastentarvikkeet. Markkinoille valmistetaan yhä älykkäämpiä leluja, jotka osaavat hyödyntää niille opetettuja asioita. Lelut muun muassa kuuntelevat puhetta ja puhuvat. Esimerkiksi itkuhälyttimiin voidaan asentaa kuvayhteys.

Erityisesti älykkäisiin IoT-laitteisiin liittyy yhä enemmän tietoturva- sekä käyttöturvavariskejä varsinkin, jos laitteiden oletussalasanat jäävät vaihtamatta tai ohjelmistopäivitykset tekemättä. Rikollisten mielenkiinto onkin kohdistumassa perinteisistä tietokoneista kodin muihin digitaalisiin laitteisiin. Mikäli joku saa hallintaansa suuren joukon heikosti suojattuja laitteita, voi hän niiden avulla toteuttaa palvelunestohyökkäyksiä lamaannuttaen internetissä olevia palveluita. Toisaalta jopa yksittäisten IoT-laitteiden saaminen haltuun voi itsessään olla arvokasta vahingoittamis- tai kiristystarkoituksessa tai vaikkapa taloudellisen rikoshyödyn tavoittelemisessa.

Tietoturvalla tarkoitetaan tietojen, palvelujen, järjestelmien ja tietoliikenteen suojaamista. Keinoja suojaamiseen ovat esimerkiksi virustorjunta, palomuuuri, tietojen salaaminen ja varmuuskopiointi, tilojen lukitus, kulunvalvonta ja varmenteiden käyttö. Vastaavasti käyttöturvallisella tietojärjestelmällä tarkoitetaan tässä selkeää järjestelmää, joka ei aiheuta fyysisiä, psyykkisiä tai taloudellisia vahinkoja normaali-, poikkeus- eikä virhetilanteissa.

Kiinteistöt ja niihin rakennetut esineiden internetiä hyödyntävät automaatiojärjestelmät voivat olla hyvin haavoittuvia, mikäli järjestelmien turvallisuutta hoidetaan huolimattomasti. Eräs esimerkki kiinteistöjen haavoittuvuudesta

löytyy vuoden 2013 lopulta, kun rikolliset murtautuivat yhdysvaltalaisen Target-kauppaketjun ilmanvaihtolaitteistoon. Laitteisto oli kytketty julkiseen internetverkkoon helpon etähallinnan vuoksi, mutta samalla se oli myös yhteydessä yrityksen maksujärjestelmäverkkoon. Tätä reittiä pitkin varastettiin kymmenien miljoonien asiakkaiden maksukorttitiedot. Internetin vahvuus on siinä, että se verkottaa laitteet toisiinsa, mutta Target-ketjun tapauksessa laitteiden kytkeminen julkiseen verkkoon oli virhe. Jos laite on liitetty internetiin huolehtimatta tietoturvasta, on mahdollista, että ilkeämielinen löytää sen ja kykenee halvaannuttamaan järjestelmän. Kriittiset järjestelmät kannattaakin eristää julkisesta internetverkosta, jotta tällaisia tapauksia ei pääse syntymään.

Kysymykset

Vastaa kysymyksiin 1.1–1.7 edellä olevan aineiston pohjalta. Vastaa omille riveille seuraaviin väittämiin kirjoittamalla joko *kyllä* tai *ei*.

Kysymys 1.1. IoT-laite on WWW-verkkoon yhteydessä oleva laite. (1 p.)

Kysymys 1.2. IoT-laite joko lähettää tai vastaanottaa tietoa. (1 p.)

Kysymys 1.3. IoT-laite ei välttämättä tarvitse omaa virtalähdettä. (1 p.)

Kysymys 1.4. IoT-laitteesta muodostuu tietoturvariski vain, jos se on yhdistetty johonkin tietoverkkoon. (1 p.)

Kysymys 1.5. IoT-laite voi olla yhteydessä muihin IoT-laitteisiin ainoastaan pilvipalveluiden kautta. (1 p.)

Kysymys 1.6. IoT:n yhtenä tavoitteena on tehdä yritysten tietojärjestelmien käyttämisestä turvallisempaa. (1 p.)

Kysymys 1.7. IoT-lelun voi huoletta yhdistää avoimeen internet-verkkoon, kunhan siihen on asetettu salasana. (1 p.)

Vastaa kysymyksiin 1.8 ja 1.9 edellä olevan aineiston ja omien tietojesi pohjalta. Vastausten arvostelussa kiinnitetään huomiota yksikäsitteisyyteen, esitystavan sujuvuuteen ja jäsennykseen sekä näkökulmien monipuolisuuteen.

Kysymys 1.8. Millaisia mahdollisuuksia esineiden internet voisi tarjota kotitalouksille? Esittele **kaksi** selkeästi erilaista esimerkkiä arjen helpottamiseksi tai tehostamiseksi IoT-laitteiden avulla. Esimerkit eivät saa olla suoraan peräisin taustamateriaalista, mutta voit johtaa omia esimerkkejä taustamateriaaliin perustuen. Ota esimerkeissäsi kantaa ainakin seuraaviin asioihin:

Tietojenkäsittelytieteen valintakoe 22.5.2017

- Millaisia IoT-laitteita ja muita esineitä esimerkki sisältää? Muut esineet voivat tässä olla tietojärjestelmiä sekä muita sähköisiä ja mekaanisia esineitä, joiden kanssa IoT-laitteet ovat vuorovaikutuksessa.
- Mitä dataa esimerkin IoT-laitteet lähettävät tai vastaanottavat? Kuvaile datan sisältö ja anna siitä esimerkki.
- Minkä kategorian IoT-laitteita esimerkissä käytetään?
- Kuvaa kunkin IoT-laitteen osalta, onko tietoliikenne yksi- vai kaksisuuntaista.

(maksimipistemäärä 10)

Kysymys 1.9. Esittele

- kaksi käyttöturvallisuushkaa (4 p.) ja
- kaksi tietoturvaluushkaa (4 p.),

joita IoT-laitteiden käytöstä voi syntyä. Kunkin uhkan kuvauksessa tulee käyttää eri IoT-laitetta tai -laitteita, eivätkä uhkat saa olla suoraan kysymyksestä 1.8. Kussakin kuvatussa uhkassa tulee esitellä kyseinen tietojärjestelmä sekä kukin sen sisältämä IoT-laite ja kunkin IoT-laitteen käyttämä viestintä yleistajuisesti. Esimerkit eivät saa olla suoraan peräisin taustamateriaalista, mutta voit johtaa omia esimerkkejä taustamateriaaliin perustuen. (maksimipistemäärä 8)