Markus Mulkahainen

Radiotaajuisen etätunnistuksen tietoturvaongelmat esineiden Internetissä

Tietotekniikan kandidaatintutkielma

23. maaliskuuta 2016

Jyväskylän yliopisto

Tietotekniikan laitos

Tekijä: Markus Mulkahainen

Yhteystiedot: markus.v.m.mulkahainen@student.jyu.fi

Ohjaaja: Sanna Mönkölä

Työn nimi: Radiotaajuisen etätunnistuksen tietoturvaongelmat esineiden Internetissä

Title in English: RFID security issues in the Internet of Things

Työ: Kandidaatintutkielma

Sivumäärä: 26+0

Tiivistelmä: Radiotaajuinen etätunnistus (RFID, engl. *radio frequency identification*) on viivakoodiin verrattavissa oleva radiotaajuuksilla toimiva etätunnistusjärjestelmä. RFID on eräs esineiden Internetin aistitason tekniikoista, ja sitä voidaan käyttää esineiden väliseen langattomaan tunnistukseen ja tiedonsiirtoon. Tutkielma esittelee tekniikkaan liittyviä tietoturvaongelmia ja mahdollisia ratkaisukeinoja. RFID-järjestelmät ovat alttiita useille hyökkäyksille, mutta niiden käytöstä voi aiheutua myös tahattomia ongelmatilanteita, muun muassa törmäyskonflikteja ja standardiongelmia. Radiotaajuisen etätunnistuksen tietoturvaongelmia voidaan pyrkiä estämään käyttämällä erilaisia tietoturvaprotokollia, joista esimerkkinä tutkielmassa esitellään SRAC-autentikointiprotokolla.

Avainsanat: Internet of Things, esineiden Internet, IoT, RFID, tietoturva, aistitaso

Abstract: Radio frequency identification (RFID) is a system similar to barcode for identifying objects over a radio frequency interface. RFID is a common technology used in Internet of Things (IoT) devices for wireless communication and unique identification. This survey explores the security issues concerning RFID and describes their severities and possible solutions. RFID-systems are vulnerable to several attacks, and the usage of RFID can cause unintentional issues such as conflict collisions and standardizing problems. Some of the security issues concerning RFID can be prevented by using security protocols, such as SRAC authentication protocol which is described in the survey.

Keywords: Internet of Things, IoT, RFID, security, perception layer

Kuviot

Sisältö

1 Johdanto

Esineiden Internet (IoT, engl. *internet of things*) tarkoittaa laajaa Internetiin yhdistettyjen esineiden verkostoa. Näitä esineitä voidaan tunnistaa, mitata tai kontrolloida Internet-verkon yli. Internetiin kytketyt esineet tuottavat jatkuvasti dataa, jota voidaan kerätä ja analysoida reaaliajassa. Tällaiseen tietojen keräämiseen liittyy paljon mahdollisuuksia, mutta toisaalta myös riskejä. Kun tietoa siirretään langattomasti laitteiden välillä, joku voi varastaa tietoa hyväksikäyttämällä laitteiden tietoturva-aukkoja.

Tietoturvan merkitystä esineiden Internetissä ei voi vähätellä. IoT:n sovellusalueet vaihtelevat teollisuudesta lääketieteeseen, ja erityisen tärkeäksi tietoturvan merkitys nousee juuri terveys- ja lääketieteen sovelluksissa. Hossain, Fotouhi ja Hasan (2015) esittävät skenaarion, jossa ilkivaltainen hyökkääjä saattaisi aiheuttaa internetiin kytketyn sydämentahdistimen käyttäjälle sydämenpysähdyksen, mikäli tietoturva-asioihin ei kiinnitetä huomiota. Jing ym. (2014) esittävät, että mikäli IoT:hen liittyviin tietoturvaongelmiin ei etsitä ratkaisua, esineiden Internetin kehitys voi rajoittua valtavasti.

RFID Journal (2016) esittelee radiotaajuisen etätunnistuksen (RFID, engl. *radio frequency identification*) teknologioina, jotka käyttävät radiotaajuuksia ihmisten tai esineiden tunnistamiseen. Yleisin tunnistusmenetelmä on tallentaa mikrosirulle yksilöivä sarjanumero, jonka siru voi lähettää antenninsa kautta RFID-lukijalle. Mikrosirua ja antennia kutsutaan RFID-tunnisteeksi tai RFID-tagiksi.

Hancke, Markantonakis ja Mayes (2010) esittävät esineiden Internetin vaativan usein esineiltään tunnistautumista, jolloin ne ovat osoitettavissa ja paikannettavissa Internet-verkon sisällä. Esineillä täytyy olla myös jokin tapa kommmunikoida jopa sellaisissa ympäristöissä, joissa Internet-yhteyttä ei ole saatavilla. Tästä syystä RFID-tekniikka on nähty yhtenä esineiden Internetin tärkeänä rakenneosana, joka mahdollistaa esineiden yksikäsitteisen tunnistautumisen ja langattoman kommunikaation.

Vaikka RFID:tä pidetään yhtenä esineiden Internetin mahdollistajana, altistaa tekniikka sen useille tietoturvaongelmille. RFID:n tietoturvaongelmat mahdollistavat ihmisten huomaamattoman seurannan ja henkilökohtaisten tietojen varastamisen (Juels 2006). RFID-järjestelmät

ovat alttiita monenlaisille hyökkäyksille, mutta tekniikan käytöstä voi aiheutua myös tahattomia häiriötilanteita, kuten törmäyskonflikteja.

Tutkielma keskittyy aistitason laitteiden tietoturvaongelmiin. Tutkimuksen pääpaino on radiotaajuiseen etätunnistukseen liittyvissä tietoturvaongelmissa, ja tutkimusmetodina käytetään systemaattista kirjallisuuskartoitusta. Luvussa 2 esitellään esineiden Internet, sen aistitaso ja joitakin sovellusalueita. Luku 3 esittelee RFID-tunnistustekniikan ja luku 4 siihen liittyviä tietoturvaongelmia. Yhteenvedossa 5 kootaan jokaisen luvun pääajatukset yhteen ja esitetään loppupäätelmät.

2 Esineiden Internet

Toistaiseksi esineiden Internetiä (IoT) ei ole määritelty yksiselitteisesti, vaan vallalla on useampia toisistaan hieman poikkeavia käsityksiä siitä, mitä termi tarkoittaa. Usein sillä viitataan joukkoon esineitä, jotka jollain tavalla käsittelevät tai tuottavat dataa ja siirtävät sitä verkon yli. Esine voisi olla esimerkiksi sateenvarjo, joka tarkastaa säätiedotuksen ja ilmoittaa sateen mahdollisuuden sytyttämällä valon sateenvarjon kädensijaan (McEwen ja Cassimally 2013). Esineeseen on tällöin liitetty sulautettu järjestelmä tai muu laite, joka kykenee kommunikoimaan valitun verkkopalvelun kanssa. Esineiden Internetiin liittyvien tietoturva-asioiden merkitystä korostaa IoT:n käytön laajentuminen yhteiskunnan eri sektoreille, joita esitellään tämän luvun lopussa.

IoT-laite on perinteisesti matalaa laskentatehoa käyttävä sulautettu järjestelmä, jolla on jokin yksinkertainen tehtävä. Tehtävä voi olla esimerkiksi tutkia roska-astian pinnan korkeutta ja päivittää tietoa keskitettyyn tietovarastoon tietyllä aikavälillä (Enevo Oy 2015), kuten Keränen (2016) on kandidaatintutkielmassaan esitellyt. Toisaalta tehtävä voi edellyttää jonkin asian suorittamista tai indikoimista mitatun tiedon perusteella. Esimerkiksi älytermostaatti mittaa huoneen ilmankosteutta ja lämpötilaa reaaliajassa sekä säätää ilmastointilaitetta lukemien perusteella (Hossain, Fotouhi ja Hasan 2015).

Esineiden Internetin arkkitehtuuria ei ole toistaiseksi standardoitu. Jing ym. (2014) jakavat IoT:n kolmeen tasoon: aisti-, kuljetus- ja sovellustasoon. Seuraavaksi esitellään ainoastaan aistitaso. Aistitaso on vastuussa informaation keräämisestä, kohteiden tunnistamisesta ja kontrolloinnista. Aistitasolla käytettyjä teknologioita ovat muun muassa RFID, WSN, RSN ja GPS.

Aistitaso on usein IoT:n näkyvin osa tavalliselle ihmiselle. Khan ym. (2012) selvittävät aistitason koostuvan aineellisista asioista ja esineistä, joiden tehtävänä on usein kerätä tietoa tai tunnistaa muita esineitä. Esineeseen kuuluu yleensä myös jonkinlainen sensori. Sensorin tyypistä riippuen aistitaso voi kerätä tietoa esimerkiksi sijainnista, lämpötilasta, orientaatiosta, liikkeestä, värähtelystä, kiihtyvyydestä tai kosteudesta. Tässä tutkielmassa IoT-laitteilla tarkoitetaan nimenomaan aistitason esineitä tai niihin liitettyjä laitteistoja.

Hossain, Fotouhi ja Hasan (2015) määrittelevät IoT-laitteen seuraavasti: ”IoT-laite koostuu sensoreista, aktuaattoreista, kommunikaatiorajapinnasta, käyttöjärjestelmistä, järjestelmän ohjelmistoista, esiasennetuista sovelluksista ja kevyistä palveluista.” (ss. 22, kirjoittajan suomentama). Heidän mukaansa Internet of Things -laitteisiin luetaan myös tietokoneet, tabletit, älypuhelimet, taulutietokoneet ja muut kädessä kannettavat sulautetut järjestelmät. IoT-laitteiden kirjoa täydentävät myös pelkät RFID-tunnisteet.

Esineiden Internetiä sovelletaan usealla yhteiskuntasektorilla, mikä lisää painetta IoT:n tietoturvaongelmien ratkaisuille. Bandyopadhyay ja Sen (2011) kertovat, että esineiden Internetiä käytetään kierrätykseen ja ympäristönsuojeluun liittyvissä sovelluksissa. Langattomia IoT-laitteita on mahdollista käyttää ajoneuvojen päästöjen mittauksissa ja monitoroimaan kierrätysmateriaalien keräämistä. RFID-tekniikoita käyttämällä on myös mahdollista vähentää elektronisen jätteen määrää, esimerkiksi tunnistamalla käytetyistä tietokoneista, puhelimista ja muista sähköisistä kuluttajatuotteista kierrätykseen sopivia komponentteja. RFID tarjoaa myös yrityksille mahdollisuuden kaluston ja tuotteiden seurantaan, mikä vähentää turhaa kuljettamista ja sitä kautta ympäristöpäästöjä.

Esineiden Internet tarjoaa monia sovelluksia terveydenhuollon alalle. Miorandi ym. (2012) esittävät skenaarion, jossa potilaat voisivat kantaa mukanaan terveydentilaa mittaavia sensoreita, jotka monitoroisivat muun muassa kehon lämpötilaa, verenpainetta ja hengitystiheyttä. Potilaiden terveydentilaa voitaisiin seurata etänä terveysasemilla, mikä mahdollistaisi nopean reagoinnin esimerkiksi hätätapauksissa. Toisaalta ihmiset voisivat myös helposti seurata omaa terveydentilaansa päälle puettavilla sensoreilla. Sensoreiden tuottamaa dataa, kuten käveltyjen askelten määrää tai kulutettua energiaa, voitaisiin monitoroida tietokoneohjelmilla, jotka kertoisivat elämäntapojen vaikutuksista terveyteen.

Atzori, Iera ja Morabito (2010) selvittävät, että RFID ja NFC (engl. *near field communication*) -tekniikoilla yrityksen toimitusketjun jokaista osa-aluetta aina tuotteen suunnittelusta kuljetukseen ja jakeluun on mahdollista seurata reaaliajassa. Yritykset voivat reagoida helposti muuttuviin markkinoihin, kun tuotetiedot ovat heti saatavilla. Tekniikoiden käyttö hyödyttää myös asiakkaita, sillä myyjät voivat tarjota asiakkailleen parempia saatavuus- ja tuotetietoja.

3 RFID

RFID Journal (2016) tarkoittaa RFID:llä (engl. *radio frequency identification*) teknologioita, jotka käyttävät radiotaajuuksia ihmisten tai esineiden tunnistamiseen. Yleisin tunnistusmenetelmä on tallentaa mikrosirulle yksilöivä sarjanumero, jonka siru voi lähettää antenninsa kautta RFID-lukijalle. Mikrosirua ja antennia kutsutaan RFID-tunnisteeksi tai RFID-tagiksi.

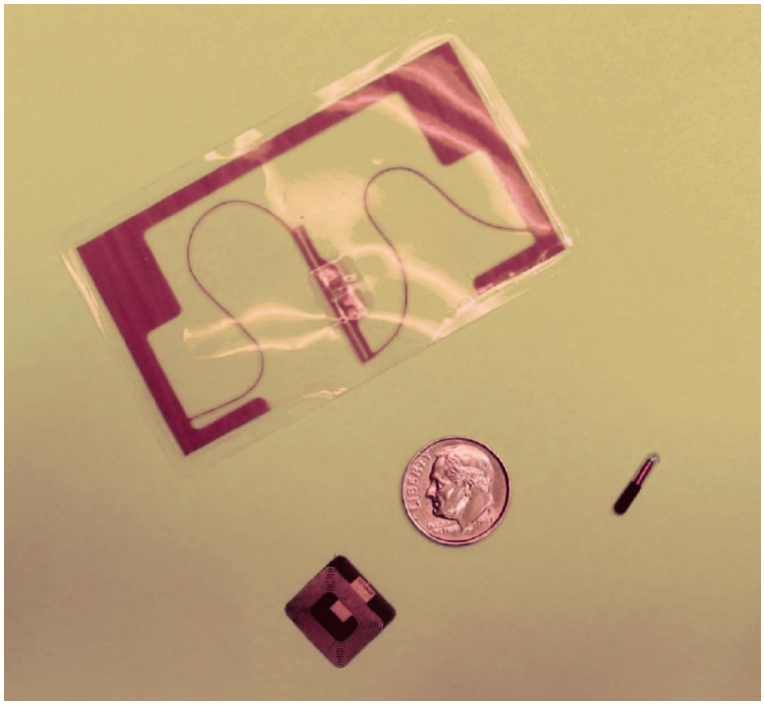
Want (2006) kertoo RFID:n olevan viivakoodiin verrattava etätunnistusjärjestelmä. Lukiessaan RFID-tunnistetta lukija ei kuitenkaan tarvitse näköyhteyttä tunnisteeseen. Lisäksi RFID tarjoaa viivakoodia suuremman joukon uniikkeja sarjanumeroita. Pelkän sarjanumeron lisäksi RFID-tunniste voi lähettää lukijalle muitakin tietoja, kuten valmistajan, tuotteen tyypin tai tiedon lämpötilasta tai muusta mitattavasta suureesta.

RFID-tunnisteista on olemassa erilaisia variaatioita, mutta erityisen mielenkiinnon kohteena ovat yleensä niin kutsutut passiiviset RFID-tunnisteet. Ne ovat pieniä ja saavat toimintaansa tarvittavan energian langattomasti RFID-lukijalta. Passiivinen RFID-tunniste on yleensä pienikokoinen joko muoviin tai lasiin koteloitu antennin ja mikrosirun yhdistelmä (kuvio 1). RFID-tunnisteita käytetään nykyään muun muassa luottokorteissa, elektronisissa passeissa, ajoneuvoissa ja villieläinten seurannassa (Juels 2006; Bonter ja Bridge 2011).

Tärkeää monelle IoT-laitteelle on tunnistaa esineitä tai tulla itse tunnistetuksi. RFID-tekniikka sopii IoT-laitteen tarvitsemaan langattomaan tiedonsiirtoon tavallisesti erittäin hyvin. Esimerkiksi kun sovelletaan RFID-tekniikkaa sairaalaympäristössä, RFID-tunnisteita voidaan käyttää potilaiden, työntekijöiden ja sairaalalaitteistojen seurantaan (Ekahau Oy; Mattila).

3.1 Toimintaperiaate

Want (2006) jakaa RFID-tunnisteet toimintatavan mukaan kahteen pääryhmään: passiivisiin ja aktiivisiin. Aktiivinen RFID-tunniste vaatii toimiakseen oman virtalähteen. Passiivisessa RFID-tunnisteessa ei ole omaa virtalähdettä, vaan se saa tarvitsemansa energian langattomasti RFID-lukijalta. Aktiivinen tunniste on passiivista RFID-tunnistetta kalliimpi, mutta toisaalta sen lukuetäisyys voi olla satoja metrejä (Juels 2006). RFID-lukija voi aktivoida



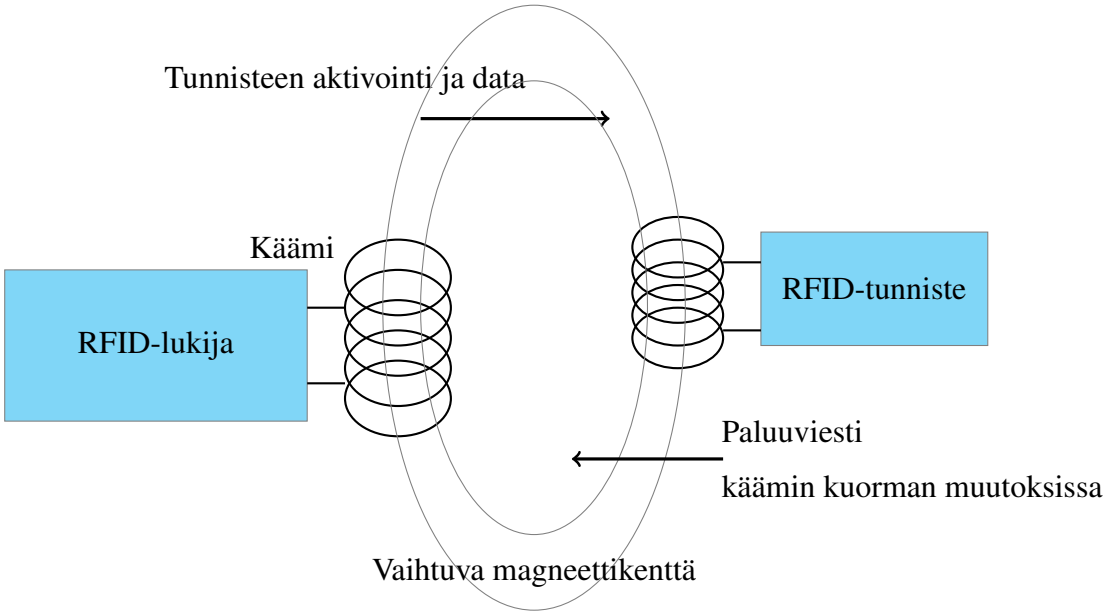
Kuvio 1. Kolme erilaista passiivista RFID-tunnistetta (Want 2006).

passiivisen RFID-tunnisteen kahdella eri tavalla, joko sähkömagneettisella induktiolla tai sähkömagneettisella säteilyllä.

Sähkömagneettisen induktion seurauksena käämiin, joka asetetaan magneettikenttään, syntyy hetkellinen sähkövirta. Jos magneettikenttä on vaihtuva, se indusoi käämiin vaihtovirran. Sama toimii myös toisin päin: kun käämiin ajetaan sähkövirtaa, se synnyttää käämin ympärille magneettikentän. Mikäli käämin sähkövirran suuntaa muutetaan jatkuvasti, syntyy vaihtuva magneettikenttä.

Chawla ja Ha (2007) kertovat, että sähkömagneettiseen induktioon perustuvat RFID-lukija ja -tunniste sisältävät käämit (kuvio 2). Sähkövirta, joka kulkee RFID-lukijan käämissä, synnyttää ympärilleen magneettikentän. Tunniste saa toimintaansa tarvittavan energian magneettikentän avulla. Klair, Chin ja Raad (2010) tarkentavat, että kun lukijan luoma vaihtuva magneettikenttä indusoi vaihtovirran RFID-tunnisteeseen, se voidaan tasasuunnata tunnisteessa tasavirraksi, jolla tunnisteen mikrosiru aktivoidaan.

Chawla ja Ha (2007) selittävät, että lukijan ja tunnisteen välinen tiedonsiirto tapahtuu kuor-



Kuvio 2. RFID-lukija aktivoi passiivisen RFID-tunnisteen synnyttämällä magneettikentän, joka luo RFID-tunnisteen käämissä sähkövirran (Chawla ja Ha 2007).

mitusmodulaatioon (engl. *load modulation*) perustuvalla mekanismilla. Kaikenlainen heilahtelu tunnisteen käämin sähkövirrassa heijastuu lukijan käämin sähkövirtaan, jonka lukija kykenee erottelemaan ja lukemaan. RFID-tunniste muuntelee sähkövirtaa vaihtelemalla kääminsä kuormitusta ja siirtää näin tietoa lukijalle.

Sähkömagneettiseen induktioon perustuva siirtotekniikka on yleensä käytössä ainoastaan lyhyen kantaman ja matalien taajuuksien RFID-laitteissa. Want (2004) esittääkin, että mitä suurempi sähkövirran muuntelutaajuus on käytössä, sitä lyhyempi on magneettikentän ulottuvuus. Esimerkiksi jos käytössä olisi 915 MHz:n taajuus, RFID-lukija ja -tunniste voisivat teoriassa sijaita korkeintaan kuuden senttimetrin päässä toisistaan, jotta kantama olisi vielä juuri ja juuri riittävä. Kantama voidaan approksimoida kaavalla

$$d = c/2\pi f, \tag{3.1}$$

missä c on valonnopeus ja f taajuus hertseinä.

Tarkemmin sanottuna kaava 3.1 jakaa käämin sähkömagneettisen kentän kahteen osaan. Kantaman sisäpuolelle jäävää aluetta kutsutaan lähikentäksi (engl. *near field region*) ja sen ulkopuolelle jäävää osaa kaukokentäksi (engl. *far field region*). Vaikka itse magneettikent-

tä ei enää ylety lähikenttää kauemmaksi, muuttuva magneettikenttä aiheuttaa kaukokentässä sähkömagneettista säteilyä (Want 2004). Mikäli laitteen vaatimuksena on pitkä etäisyys ja korkea kantoaallon taajuus, voidaan passiivisen RFID-tunnisteen aktivoimiseksi ja tiedon siirtämiseksi käyttää sähkömagneettista säteilyä. Tällöin RFID:n implementaatio muuttuu hieman (kuvio 3).

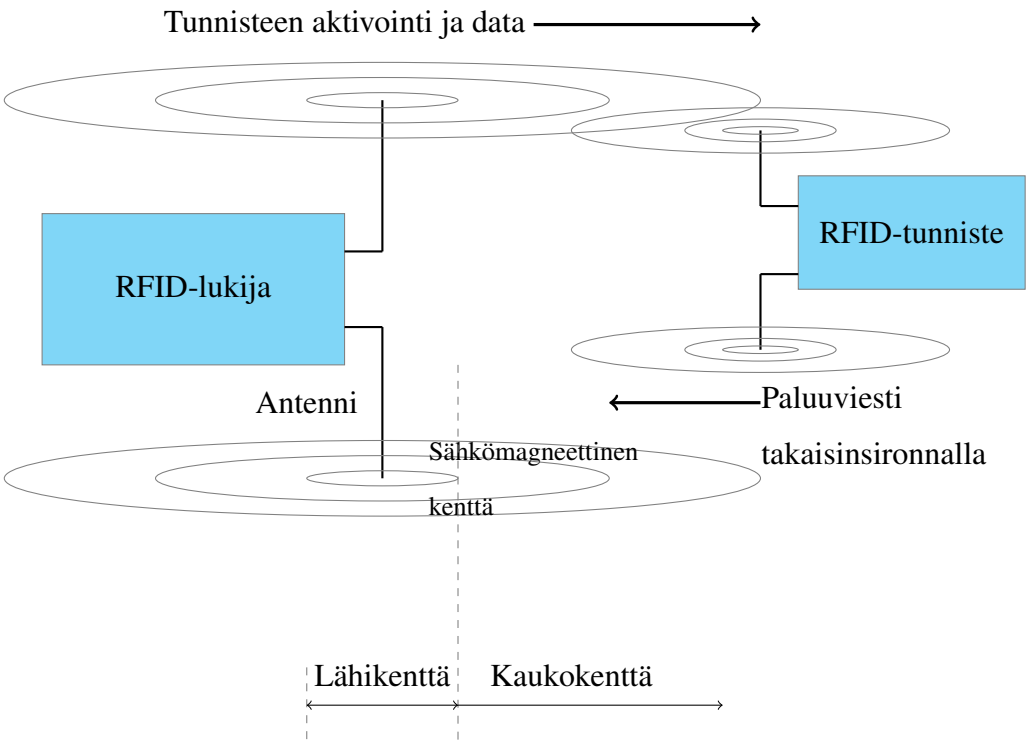
Klair, Chin ja Raad (2010) kertovat sähkömagneettiseen säteilyyn perustuvan RFID-lukijan ja tunnisteen kytkennän toimivan UHF:n (engl. *ultra high frequency*) ja mikroaaltojen taajuusalueilla. Lukijan antenni lähettää tunnisteelle jatkuvaa sähkömagneettista aaltoa, joka aiheuttaa tunnisteen dipoliantennissa potentiaalieron. Tätä potentiaalieroa käytetään tunnisteen mikrosirun aktivoimisessa.

Want (2004) selittää, että RFID-tunniste kommunikoi lukijan kanssa käyttäen niin kutsuttua takaisinsirontaa (engl. *backscattering*). Takaisinsironnassa tunniste muuntelee antenninsa impedanssia, mikä saa saapuvan säteilyn heijastumaan takaisin joko voimakkaammin tai heikommin. Lukija kykenee herkällä vastaanottimellaan lukemaan heijastuvan signaalin amplitudin muutokset ja tulkitsemaan tunnisteen paluuviestin.

3.2 Useita standardeja

RFID-tunnisteen lukemiseksi on useita erilaisia standardeja, mutta yhtä kaikkialla toimivaa kansainvälistä standardia ei ole olemassa. Jing ym. (2014) kertovat, että yhtenäisen standardin puutteesta voi aiheutua lukijan ja tunnisteen yhteensopivuusongelmia. Seurauksena voi olla esimerkiksi tilanteita, joissa lukija ei saa muodostettua yhteyttä tunnisteeseen tai lukuprosessissa voi ilmetä muita ongelmia.

RFID-tunnisteratkaisuiksi on käytetty useampia taajuusalueita ja standardeja. Näistä Want (2004) mainitsee 13,56 MHz taajuudella operoivan ISO 14443 - ja 915 MHz:n taajuudella operoivan EPCglobal-standardin, joita on molempia käytetty suurten yritysten RFID-ratkaisuissa. Yhteneväisen RFID-standardin luomisen esteenä ovat muun muassa maakohtaiset taajuusalueiden käytön rajoitteet ja yrityskohtaiset päätökset. Taajuusalueen lisäksi RFID-standardi määrittelee ilmarajapinnan, kommunikaatioprotokollan, kaistanleveyden sekä törmäyskonflikteihin ja tietoturvaan liittyviä mekanismeja (Knospe ja Pohl 2004).



Kuvio 3. RFID-lukija aktivoi passiivisen RFID-tunnisteen sähkömagneettisella säteilyllä (Chawla ja Ha 2007, mukaellen).

Want (2004) esittää standardointiongelman ratkaisuksi RFID-lukijoita, jotka voisivat operoida useamman standardin mukaisesti. Lukija voisi esimerkiksi etsiä eri taajuusalueilla toimivia tunnisteita skannaamalla, tai lukijat voisivat olla ohjelmoitavia, jolloin niitä voitaisiin sopeuttaa esimerkiksi maakohtaisiin taajuusrajoitteisiin.

4 Tietoturvaongelmia

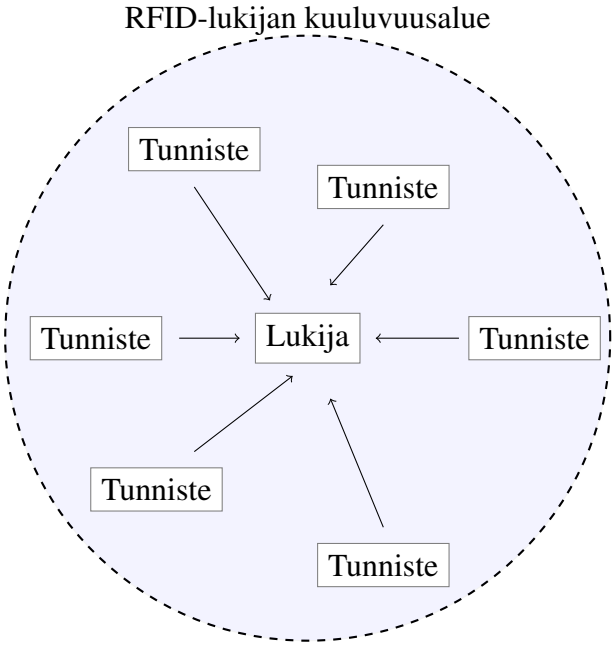
Ensimmäisiä RFID-tekniikkaa muistuttavia laitteita valmistettiin sotilaskäyttöön jo 1940-luvulla. Laitteita käytettiin vihollisko neiden erottamiseen omista lentokoneista. Vasta vuonna 1999 RFID:tä ehdotettiin ensimmäistä kertaa yksittäisten tavaroiden seurantaan toimitusketjuissa (Hancke, Markantonakis ja Mayes 2010). Nyt RFID-tekniikkaa käytetään monissa esineiden Internetin sovelluksissa, ja uusien käyttökohteiden myötä tietoturvaongelmista on tullut eri tavalla ajankohtaisia ja niiden ratkaisemisesta yhä tärkeämpää.

RFID-tekniikoiden käyttämisestä voi seurata tahattomia häiriötilanteita, kuten standardiongelmia ja törmäyskonflikteja. Lisäksi joskus metallit heijastavat radiotaajuuksia niin, että RFID-tunnisteen lukeminen häiriintyy (Juels 2006). Toinen tahaton ongelmatilanne voi syntyä RFID-tunnisteen tietynlaisesta orientaatiosta RFID-lukijan suhteen. Mikäli tunnisteen antenni on kohtisuorassa lukijan antenniin, se ei kykene vastaanottamaan lukijan lähettämää radiosignaalia (Wu ym. 2006).

RFID-järjestelmät ovat alttiita monenlaisille aktiivisille hyökkäyksille, joista muutamia käydään läpi luvussa 4.3. Lukas Grunwald esitteli vuonna 2004 RF Dump -nimisen Java-ohjelman, joka pystyi lukemaan ja muuttamaan RFID-tunnisteen tietoja tietokoneen sarjaporttiin kytketyn RFID-lukijan avulla (Lindstrom ja Thornton 2005). Tämäntyyppisten tietoturva-aukkojen korjaaminen on erityisen tärkeää, etteivät hyökkääjät saisi toteuttaa aikomuksiaan lähes vapain käsin. Alhaisten kustannusvaatimuksien ja laskentatehon takia RFID-järjestelmien tietoturvaprotokollien toteuttaminen ei kuitenkaan ole triviaalia.

4.1 Törmäyskonfliktit

Jing ym. (2014) kertovat, että törmäyskonflikti (engl. *conflict collision*) voi syntyä tilanteessa, jossa RFID-lukijan kantaman sisäpuolella on useita RFID-tunnisteita (kuvio 4). Kun useat tunnisteet lähettävät tietonsa lukijalle yhtä aikaa, voi lukija tulkita tunnisteiden tiedot virheellisesti. Törmäyskonfliktit tuhlaavat myös kaistaa ja energiaa (Klair, Chin ja Raad 2010).



Kuvio 4. Törmäyskonflikti voi syntyä tilanteessa, jossa RFID-lukijan kantaman sisäpuolella on useita RFID-tunnisteita (Klair, Chin ja Raad 2010, mukaellen).

Want (2004) selittää, että tunnisteiden törmäyskonfliktien estämiseksi on luotu erilaisia protokollia, jotka pyrkivät vähentämään tietojen lähettämistä yhtä aikaa. Tunnisteen lähetysvastetta voidaan muutella esimerkiksi ID-numeron perusteella. Tunnisteen törmäyskonfliktin riskiä pienentää myös korkea lähetystaajuus, jolloin RFID-tunnisteen tietojen lähettämiseen kuluva aika on lyhyempi. Tällöin usean tunnisteen yhtäaikaiset lähetykset osuvat epätodennäköisemmin päällekkäin.

Jing ym. (2014) tarkoittavat RFID-lukijoiden törmäyskonfliktilla tilannetta, jossa kahden tai useamman lukijan kantaman leikkausalueen sisäpuolella sijaitsee tunnisteita. Tällöin sama tieto voidaan lukea useamman lukijan kautta, jolloin tiedosta tulee toistuvaa, ja se kuormittaa kuljetuskerrosta. Voi olla myös mahdollista, että tunniste ei kykene lukijoiden törmäyskonfliktissa vastaamaan yhdellekään lukijalle (Wang, Wang ja Zhao 2006).

Wang, Wang ja Zhao (2006) jakavat lukijoiden törmäyskonfliktien ratkaisut karkeasti näkyvyyspohjaisiin (engl. *coverage based*) ja aikapohjaisiin (engl. *scheduling based*) ratkaisuihin. Näkyvyyspohjaiset ratkaisut pyrkivät minimoimaan lukijoiden päällekkäisiä ulottuvuusalueita. Tähän vaaditaan yleensä erillinen keskussolmu, joka laskee ja säätää vierekkäis-

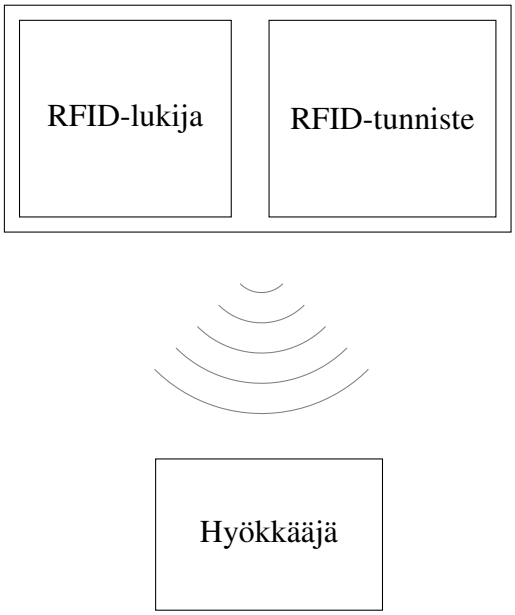
ten lukijoiden päällekkäisiä alueita, mikä lisää RFID-systeemin monimutkaisuutta ja hintaa. Aikapohjaiset ratkaisut pyrkivät taas estämään esimerkiksi lukijoiden yhtäaikaisia lähetyksiä. Tämä kuitenkin vaatii systeemiltä kykyä pitää yllä tietoa lukijoiden muodostamasta verkosta, mikä voi hidastaa systeemiä ja kuluttaa enemmän energiaa.

4.2 Salakuuntelu

RFID toimii radioaalloilla, mihin liittyy aina salakuuntelun (engl. *eavesdropping*) riski (Lindstrom ja Thornton 2005). Weis (2007) arvelee, että vakoilu ja yksityisyyden ongelmat ovat mahdollisesti RFID-systeemien suurimmat uhat. Sitä mukaa kun RFID-tekniikoita integroidaan yritysten tarjontaketjuihin ja varastojen valvontainfrastruktuureihin, siirretään myös arkaluontoista tietoa RFID-tunnisteisiin. Kuluttajatuotteissa olevien tunnisteiden vakoilu voisi aiheuttaa arkaluontoisen tiedon vuotoja ja yksittäisten henkilöiden seurantaa.

Salakuuntelutilanteessa hyökkääjä sieppaa RFID-lukijan ja -tunnisteen välistä kommunikaatiota yhteensopivalla lukijalla (kuvio 5). Mohite, Kulkarni ja Sutar (2013) kertovat, että salakuuntelu on helppoa ja tehokasta, sillä RFID-järjestelmät käyttävät viestittelyyn salaamatonta liikennettä, mikä johtuu tunnisteiden muisti- ja hintarajoitteista. Hyökkääjän tavoitteena voi olla esimerkiksi siepata yksittäiseen henkilöön liittyvää tietoa, mutta tavoitteena voi olla myös hyödyntää siepattua tietoa seuraavassa hyökkäyksessä. Siepattua tietoa voitaisiin käyttää niin sanottuun toistohyökkäykseen (engl. *replay attack*), jossa hyökkääjä käyttää samoja tietoja esittääkseen olevansa joko vastaava tunniste tai lukija.

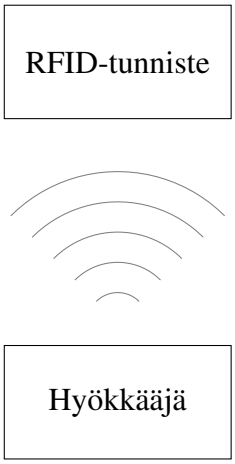
Radioaallot voivat liikkua yllättävillä tavoilla, ja signaali voi yltää monta kertaa kauemmaksi kuin sen maksimikantaman on ajateltu yltävän (Lindstrom ja Thornton 2005). Juels (2006) jakaakin passiivisten RFID-tunnisteiden lukuetäisyydet neljään kategoriaan. Nominaalilukuetäisyys (engl. *nominal read range*) tarkoittaa RFID-standardin ja tuotespesifikaation esittämää tunnisteen lukuetäisyyttä, joka saavutetaan tavallisella RFID-lukijalla, antennilla ja antoteholla siten, että tunniste on luotettavasti aktivoitavissa ja luettavissa. Nominaalietäisyyden voi ylittää poikkeava lukuetäisyys (engl. *rogue scanning range*), joka saavutetaan herkällä RFID-lukijalla, tehokkaalla antennilla tai antennijoukolla ja mahdollisesti suurella antoteholla.



Kuvio 5. Hyökkääjä sieppaa RFID-lukijan ja -tunnisteen välistä liikennettä (Hancke 2008, mukaellen).

Tunnisteen salakuunteluetäisyys (engl. *tag-to-reader eavesdropping range*) tarkoittaa maksimietäisyyttä, jossa lukijan aktivoimaa tunnistetta voidaan salakuunnella toisella lukijalla. Tunnisteen salakuunteluetäisyys voi olla poikkeavaa lukuetäisyyttä suurempi, sillä sen ei tarvitse aktivoida tunnistetta. Lukijan salakuunteluetäisyys (engl. *reader-to-tag eavesdropping range*) tarkoittaa vastaavasti maksimietäisyyttä, jossa lukijaa voidaan salakuunnella. Lukijan salakuunteluetäisyys on tunnisteen lukuetäisyyttä huomattavasti suurempi, mahdollisesti jopa kilometrien mittainen, sillä RFID-lukijat lähettävät dataa suuremmalla teholla kuin RFID-tunnisteet.

Vakoilu ei välttämättä ole passiivista, vaan hyökkääjä voi myös aktiivisesti skannata, tai niin sanotusti varastaa (engl. *skimming*), tunnisteesta tietoa omalla lukijallaan (kuvio 6) (Weis 2007). Heydt-Benjamin ym. (2007) tekivät kokeen, jossa he ohjelmoivat tavallisen RFID-lukijan emuloimaan luottokorttien lukemiseen tarkoitettua RFID-lukijaa. Koe osoittaa, että luottokorttien RFID-tunnisteet vastaavat emuloidulle RFID-lukijalle täsmälleen samalla tavalla kuin oikealle luottokorttien RFID-lukijalle. Luottokorteissa ei käytetä minkäänlaista turvajärjestelmää tunnistamaan valtuutettua RFID-lukijaa, ennen arkaluonteisten tietojen lähettämistä.



Kuvio 6. Hyökkääjä varastaa (engl. *skimming*) RFID-tunnisteesta tietoa mahdollisesti väärennetyllä RFID-lukijalla (Hancke 2008, mukaellen).

Edenfield (2007) kuvaa patentissaan suojastusta (engl. *shielding*) hyödyntäviä koteloita ja lompakoita, joissa voitaisiin säilyttää RFID-tunnisteita sisältäviä tavaroita. Koteloa ympäröi ohut metallikerros, joka vaimentaa sähkömagneettista säteilyä niin, että kotelon sisältäviä RFID-tunnisteita on mahdotonta aktivoida tai lukea ulkopuolelta. Tämä tekisi tietojen varastamisen kuviossa 6 esitetyllä tavalla mahdottomaksi.

4.3 Hyökkäykset ilmarajapinnan yli

Lindstrom ja Thornton (2005) tarkoittavat ilmarajapinnalla (engl. *air-interface*) RFID-lukijan ja -tunnisteen väliin jäävää radiotaajuuksilla toimivaa kommunikaatiorajapintaa. He kategorisoivat ilmarajapinnan yli tapahtuvat hyökkäykset karkeasti neljään osaan: huijauksiin (engl. *spoofing*), injektioihin (engl. *insert attack*), toistohyökkäyksiin (engl. *replay attack*) ja palvelunestohyökkäyksiin (DOS, engl. *denial of service*).

Huijauksessa (engl. *spoofing*) on tarkoituksena syöttää RFID-systeemiin väärää informaatiota siten, että väärennetty tieto hyväksytään järjestelmään (Lindstrom ja Thornton 2005). Lee ym. (2005) antavat esimerkin huijauksesta, jossa hyökkääjä vaihtaa jonkin myytävän tuotteen RFID-tunnisteen toiseen, joka viittaakin halvempaan tavaraan. Seurauksena automaattinen myyntipöytä veloittaisi hyökkääjää halvemmasta tuotteesta. Heidän mukaansa lukijan ja tunnisteen välinen autentikointi on avainasemassa huijauksien estämisessä.

Rieback ym. (2006) esittävät, että RFID-lukija olettaa RFID-tunnistetta lukiessaan saapuvan datan olevan ennalta määrätyssä muodossa. Hyökkääjä voisi injektoida tunnisteen paluuviestiin esimerkiksi jonkin haitallisen systeemikomennon, joka voi turmella RFID-lukijan taustaohjelmistoja (engl. *back-end software*). Injektiohyökkäys voitaisiin toteuttaa käyttämällä perinteistä SQL-injektiota, jossa tunnisteeseen asetetaan jokin SQL-kielinen lause, kuten *;shutdown–*, joka sammuttaisi RFID-systeemin taustalla pyörivän tietokantainstanssin (Rieback, Crispo ja Tanenbaum 2006).

Mohite, Kulkarni ja Sutar (2013) esittävät toistohyökkäyksen (engl. *replay attack*) eräänlaisena identiteettivarkautena, jossa hyökkääjä syöttää RFID-lukijalle uhrin RFID-tunnistetta vastaavia tietoja. Toistohyökkäys voi olla seurausta salakuuntelusta (katso luku 4.2) tai RFID-tunnisteen kloonauksesta. Toistohyökkäys vaatii ensin hyökkäyksen kohteena olevan RFID-tunnisteen tietojen selvittämistä jollakin keinolla.

Heydt-Benjamin ym. (2007) käyttivät toistohyökkäyskokeessaan pientä mikroprosessorin sisältämää laitetta, joka pystyi lähettämään tietoa radioteitse ISO 14443-B -standardin mukaisesti. He ohjelmoivat laitteen niin, että se kykeni kommunikoimaan kaupallisten luottokorttien lukemiseen tarkoitettujen RFID-lukijoiden kanssa. Tämän jälkeen he ohjelmoivat luottokorttiemulaattorin vastaamaan lukijalle käyttäen aiemmin varastamiensa oikeiden luottokorttien tietoja (katso luvun 4.2 loppu). Kokeessa kaupalliset luottokorttien RFID-lukijat eivät kyenneet tunnistamaan ja erottamaan luottokorttiemulaattoria oikeista luottokorteista.

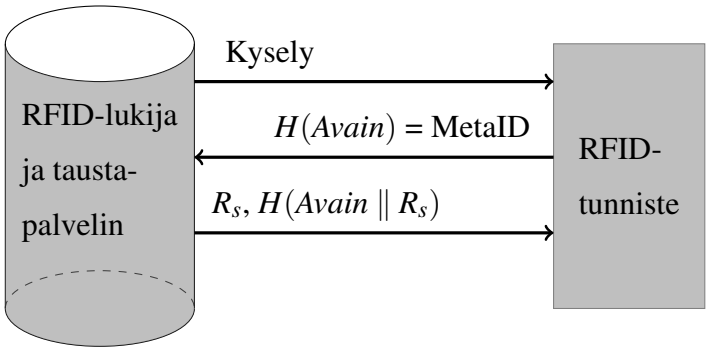
Mohite, Kulkarni ja Sutar (2013) kertovat, että palvelunestohyökkäykset radiotaajuisia laitteita vastaan perustuvat yleensä radiohäirintään (engl. *jamming*). Sen tarkoituksena on aiheuttaa laitteen taajuusalueella sellaista häiriösignaalia, joka täyttää ilmarajapinnan ja lamauttaa RFID-systeemin viestiyhteydet. Voimakkaat sähkömagneettiset signaalit voivat pahimmillaan aiheuttaa laitteissa myös fyysisiä vahinkoja (Weis 2007).

Palvelunestohyökkäys voi perustua myös suojastukseen (engl. *shielding*). RFID-lukijan tai -tunnisteen antenni voitaisiin esimerkiksi kääriä metallikalvoon, mikä estää lukijan ja tunnisteen välisen yhteyden (Finkenzeller 2009). Samaa menettelyä voidaan käyttää myös suojautumistarkoituksessa (katso luvun 4.2 loppu).

Mikäli RFID-tunniste vastaa lukijan kyselyihin aina vakioarvolla, on tunnisteen seuranta ja

kloonaaminen helppoa. Se voidaan kuitenkin estää jollakin RFID-autentikointiprotokollalla. Protokolla tarjoaa yleensä kaksisuuntaisen tunnistuksen (engl. *mutual authentication*), mikä tarkoittaa sitä, että tunniste autentikoi lukijan ja lukija autentikoi tunnisteen. Lee ym. (2005) kertovat, että RFID-tunnisteen laskentateho, tallennustila ja kommunikointikyky ovat rajalliset, ja siksi RFID-tunnisteen autentikointia ei voida toteuttaa samalla tavoin kuin muissa järjestelmissä.

Lee ja Verbauwhede (2005) esittävät tutkimuksessaan tunnisteen kloonaamisen ja seuraamisen estämiseksi SRAC-autentikointiprotokollaa (engl. *semi-randomized access control*, kuvio 7). SRAC ei ole ainut eikä edes uusin autentikointiprotokolla tämän kandidaatintutkielman kirjoitushetkellä, mutta se on tarpeeksi yksinkertainen toimimaan esimerkkinä. Protokollat ovat aina enemmän tai vähemmän toistensa kaltaisia, mistä syystä muiden autentikointiprotokollien implementaatiot muistuttavat SRAC-protokollaa.



1. Lukija lähettää tunnisteelle kyselyn.

2. Tunniste lähettää MetaID:n lukijan kautta palvelimelle.

3. Palvelin selvittää *Avaimen* MetaID:n perusteella, generoi satunnaisluvun R_s
ja tarkistaa, olisiko $H(Avain \oplus R_s)$ uniikki MetaID.
Mikäli ei, R_s generoidaan uudestaan niin kauan, kunnes $H(Avain \oplus R_s)$ on uniikki.
Palvelin päivittää *Avaimen* seuraavasti:

```
if (H(Avain_nyk) == MetaID) {
   Avain_edell = Avain_nyk
   Avain_nyk = H(Avain_nyk ⊕ R_s)
}
else if (H(Avain_edell) == MetaID) {
   Avain_nyk = H(Avain_edell ⊕ R_s)
}
Avain = Avain_edell
```

H: yksisuuntainen hash-funktio
$\oplus$: XOR-bittioperaatio
$\parallel$: ketjutusoperaattori

Palvelin lähettää tiedot R_s ja $H(Avain \parallel R_s)$ lukijan kautta tunnisteelle.

4. Tunniste tarkastaa $H(Avain \parallel R_s)$:n oikeellisuuden.
Jos tieto on oikein, tunniste tallentaa *Avaimen* arvoksi $H(Avain \oplus R_s)$.

Kuvio 7. SRAC-protokollaa käytetään RFID-lukijan ja -tunnisteen väliseen autentikointiin. SRAC-protokolla ei anna täydellistä suojaa toistohyökkäystä vastaan. (Lee ja Verbauwhede 2005, mukaellen)

5 Yhteenveto

Esineiden Internet on yksi digitalisoituvan maailman peruspilareista. Sitä hyödynnetään muun muassa teollisuuden, kuljetuksen, energiateollisuuden, jälleenmyynnin ja terveydenhuollon sektoreilla. IoT:n kehityksen haasteina ovat esimerkiksi Internetin arkkitehtuurin rajoitteet, hajanaisten sovellusten, ympäristöjen ja laitteiden hallinta sekä tietoturvaongelmat (Bandyopadhyay ja Sen 2011). Tietoturvan puutteet esineiden Internetissä aiheuttavat yksityisyysongelmia tai pahimmissa skenaarioissa henkilövahinkoja.

Radiotaajuinen etätunnistus tarjoaa esineiden Internetin laitteille yksikäsitteisen tunnistautumiskeinon ja mahdollisuuden langattomaan tiedonsiirtoon jopa sellaisissa ympäristöissä, joissa internet-yhteyttä ei ole saatavilla. Esineiden Internetin aistitasolla käytettyyn tekniikkaan liittyy kuitenkin tietoturvaongelmia, joihin on syytä etsiä ratkaisuja. RFID-järjestelmiä on esimerkiksi mahdollista salakuunnella tuotespesifikaation ilmoittaman maksimikantaman ulkopuolella. Järjestelmiä vastaan voidaan myös hyökätä useilla tavoilla. Aktiivisia hyökkäyksiä ovat muun muassa varastamiset (engl. *skimming*), huijaukset (engl. *spoofing*), toistohyökkäykset (engl. *replay attack*), injektiot (engl. *insert attack*) ja palvelunestohyökkäykset (engl. *denial of service*). Hyökkäyksiä voidaan yrittää estää erilaisilla tietoturvaprotokollilla.

Toisistaan poikkeavien RFID-implementaatioiden suuri määrä altistaa jo yksin RFID-järjestelmiä tietoturvaongelmille, sillä yhtenäistä ja kaikkialla toimivaa RFID-standardia ei ole olemassa. Muita tahattomia tietoturvaongelmia ovat törmäyskonfliktit, jotka johtuvat joko RFID-tunnisteiden suuresta lukumäärästä yhden lukijan kantaman sisäpuolella tai usean lukijan päällekkäisestä kuuluvuusalueesta. Radiotaajuisen etätunnistuksen tietoturvaratkaisujen haasteina ovat alhaiset kustannusvaatimukset sekä tunnisteiden matala laskentateho. RFID jatkaa voittokulkuaan yhtenä esineiden Internetin tärkeänä mahdollistajana, mutta kehitystyötä sen tietoturvaongelmien ratkaisemiseksi on jatkettava.

Lähteet

Atzori, L., A. Iera ja G. Morabito. 2010. “The Internet of Things: A survey”. *Computer Networks* 54 (15): 2787–2805. ISSN: 1389-1286. doi:http://dx.doi.org/10.1016/j.comnet.2010.05.010. http://www.sciencedirect.com/science/article/pii/S1389128610001568.

Bandyopadhyay, D., ja J. Sen. 2011. “Internet of Things: Applications and Challenges in Technology and Standardization”. *Wireless Personal Communications* 58 (1): 49–69. http://dx.doi.org/10.1007/s11277-011-0288-5.

Bonter, D. N., ja E. S. Bridge. 2011. “Applications of radio frequency identification (RFID) in ornithological research: a review”. *Journal of Field Ornithology* 82 (1): 1–10.

Chawla, V., ja D. S. Ha. 2007. “An overview of passive RFID”. *Communications Magazine, IEEE* 45 (9): 11–17.

Edenfield, B. 2007. *Card cases and wallets with radio frequency shielding.* US Patent App. 11/281,543, toukokuu. https://www.google.com/patents/US20070109130.

Ekahau Oy. *Real-Time Location Tracking.* Saatavilla WWW-muodossa, http://www.ekahau.com/real-time-location-system/solutions/healthcare/asset-tracking-management, viitattu 05.02.2016.

Enevo Oy. 2015. *WE-008 sensor datasheet.* Saatavilla WWW-muodossa, http://cdn3.enevo.com/wp-content/uploads/2015/03/20135358/Enevo-Datasheet-WE-008-A4-English-web1.pdf, viitattu 15.02.2016.

Finkenzeller, K. 2009. “Known attacks on RFID systems, possible countermeasures and upcoming standardisation activities”. Teoksessa *5th European Workshop on RFID Systems and Technologies.*

Hancke, G. 2008. “Eavesdropping attacks on high-frequency RFID tokens”. Teoksessa *4th Workshop on RFID Security (RFIDSec),* 100–113.

Hancke, G., K. Markantonakis ja K. Mayes. 2010. “Security Challenges for User-Oriented RFID Applications within the"Internet of Things"”. *Journal of Internet Technology* 11 (3): 307–313.

Heydt-Benjamin, T. S., D. V. Bailey, K. Fu, A. Juels ja T. O’Hare. 2007. “Financial Cryptography and Data Security: 11th International Conference, FC 2007, and 1st International Workshop on Usable Security, USEC 2007, Scarborough, Trinidad and Tobago, February 12-16, 2007. Revised Selected Papers”. Luku Vulnerabilities in First-Generation RFID-enabled Credit Cards, toimittanut S. Dietrich ja R. Dhamija, 2–14. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-540-77366-5. doi:10.1007/978-3-540-77366-5_2. http://dx.doi.org/10.1007/978-3-540-77366-5_2.

Hossain, M. M., M. Fotouhi ja R. Hasan. 2015. “Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things”. Teoksessa *Services (SERVICES), 2015 IEEE World Congress on,* 21–28.

Jing, Q., A. V. Vasilakos, J. Wan, J. Lu ja D. Qiu. 2014. “Security of the Internet of Things: perspectives and challenges”. *Wireless Networks* 20 (8): 2481–2501. http://dx.doi.org/10.1007/s11276-014-0761-7.

Juels, A. 2006. “RFID security and privacy: a research survey”. *Selected Areas in Communications, IEEE Journal on* 24 (2): 381–394.

Keränen, J. 2016. *Tiedonkeruun hallinta esineiden internetissä.*

Khan, R., S. U. Khan, R. Zaheer ja S. Khan. 2012. “Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges”. Teoksessa *Frontiers of Information Technology (FIT), 2012 10th International Conference on,* 257–260.

Klair, D. K., K.-W. Chin ja R. Raad. 2010. “A Survey and Tutorial of RFID Anti-Collision Protocols”. *Communications Surveys & Tutorials, IEEE* 12 (3): 400–421.

Knospe, H., ja H. Pohl. 2004. “RFID security”. *Information Security Technical Report* 9 (4): 39–50. ISSN: 1363-4127. doi:http://dx.doi.org/10.1016/S1363-4127(05)70039-X. http://www.sciencedirect.com/science/article/pii/S136341270570039X.

Lee, S. M., Y. J. Hwang, D. H. Lee ja J. I. Lim. 2005. “Computational Science and Its Applications – ICCSA 2005: International Conference, Singapore, May 9-12, 2005, Proceedings, Part I”. Luku Efficient Authentication for Low-Cost RFID Systems, toimittanut O. Gervasi, M. L. Gavrilova, V. Kumar, A. Laganà, H. P. Lee, Y. Mun, D. Taniar ja C. J. K. Tan, 619–627. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-540-32043-2. doi:10.1007/11424758_65. http://dx.doi.org/10.1007/11424758_65.

Lee, Y. K., ja I. Verbauwhede. 2005. “Secure and Low-cost RFID Authentication Protocols”. Teoksessa *2nd IEEE International Workshop on Adaptive Wireless Networks (AWiN 2005).* IEEE. https://www.cosic.esat.kuleuven.be/publications/article-663.pdf.

Lindstrom, P., ja F. Thornton. 2005. *RFID Security.* ID: 10120306. Rockland, MA, USA: Syngress Publishing, marraskuu. ISBN: 9780080489650.

Mattila, R. *Saako potilaaseen panna paikannuslaitteen? Alysairaala herattaa eettisia kysymyksia.* Saatavilla WWW-muodossa, http://yle.fi/uutiset/saako_potilaaseen_panna_paikannuslaitteen_alysairaala_herattaa_eettisia_kysymyksia/8624457, viitattu 05.02.2016.

McEwen, A., ja H. Cassimally. 2013. *Designing the Internet of Things.* Oxford, GBR: John Wiley & Sons, lokakuu. ISBN: 9781118430637.

Miorandi, D., S. Sicari, F. D. Pellegrini ja I. Chlamtac. 2012. “Internet of things: Vision, applications and research challenges”. *Ad Hoc Networks* 10 (7): 1497–1516. http://www.sciencedirect.com/science/article/pii/S1570870512000674.

Mohite, S., G. Kulkarni ja R. Sutar. 2013. “RFID Security Issues”. Luku 9 (September-2013) teoksessa *International Journal of Engineering Research and Technology,* nide 2. ESRSA Publications.

RFID Journal. 2016. *What is RFID?* Saatavilla WWW-muodossa, http://www.rfidjournal.com/faq/show?49, viitattu 03.02.2016.

Rieback, M. R., B. Crispo ja A. S. Tanenbaum. 2006. “Is your cat infected with a computer virus?” Teoksessa *Pervasive Computing and Communications, 2006. PerCom 2006. Fourth Annual IEEE International Conference on,* pages. Maaliskuu. doi:10.1109/PERCOM.2006.32.

Rieback, M. R., P. N. Simpson, B. Crispo ja A. S. Tanenbaum. 2006. “RFID malware: Design principles and examples”. Special Issue on PerCom 2006, *Pervasive and Mobile Computing* 2 (4): 405–426. ISSN: 1574-1192. doi:http://dx.doi.org/10.1016/j.pmcj.2006.07.008. http://www.sciencedirect.com/science/article/pii/S157411920600040X.

Wang, D., J. Wang ja Y. Zhao. 2006. “A Novel Solution to the Reader Collision Problem in RFID System”. Teoksessa *Wireless Communications, Networking and Mobile Computing, 2006. WiCOM 2006.International Conference on,* 1–4.

Want, R. 2006. “An introduction to RFID technology”. ID: 1, *Pervasive Computing, IEEE* 5 (1): 25–33.

Want, R. 2004. “The Magic of RFID”. *Queue* (New York, NY, USA) 2, numero 7 (lokakuu): 40–48. doi:10.1145/1035594.1035619. http://doi.acm.org/10.1145/1035594.1035619.

Weis, S. A. 2007. “RFID (radio frequency identification): Principles and applications”. *System* 2:3 Principles.

Wu, N., M. Nystrom, T. Lin ja H. Yu. 2006. “Challenges to global RFID adoption”. *Technovation* 26 (12): 1317–1323. ISSN: 0166-4972. http://www.sciencedirect.com/science/article/pii/S016649720500146X.