Heli Kallio

Lääkintälaitteiden kyberturvallisuuden standardit ja testaaminen

Tietotekniikan pro gradu -tutkielma

17. elokuuta 2017

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Heli Kallio

Yhteystiedot: heli.m.kallio@jyu.fi

Ohjaajat: Timo Hämäläinen ja Tiina Kovanen

Työn nimi: Lääkintälaitteiden kyberturvallisuuden standardit ja testaaminen

Title in English: The standards and testing of the cyber security of medical devices

Työ: Pro gradu -tutkielma

Suuntautumisvaihtoehto: Tietoliikenne

Sivumäärä: 77+0

Tiivistelmä: Tietotekniikkaa sisältävät lääkintälaitteet pitävät meidät hengissä, jos kehomme pettää. Esimerkiksi ostoskeskuksissa olevat älykkäät defibrillaattorit antavat maallikoillekin mahdollisuuden antaa tehokasta ensiapua sydänkohtaukseen. Tietotekniikan käyttäminen lääkintälaitteissa tuo mahdollisuuksien lisäksi uhkia. Tässä tutkielmassa perehdytään siihen, miten standardit ja testaaminen edistävät kyberturvallisuutta, uhkien torjumista. Ensin tehdään katsaus kirjallisuuteen ja standardeihin ja sitten kytketään tieto käytäntöön testaamalla potilasmonitoria kirjallisuuden pohjalta.

Tulos oli, että tutkittava potilasmonitori oli hyvin avoin fyysisen käyttöliittymän kautta. Esimerkiksi potilastiedot olivat saatavilla ja muokattavissa kirjautumatta. Tietoliikenneyhteyksien kautta laitteeseen ei juurikaan saatu yhteyttä. Monitori läpäisi osan kirjallisuudesta valituista vaatimuksista. Muutaman vaatimuksen täyttämisestä ei voida olla varmoja, sillä kehittäjille oli annettu niiden suhteen valinnanvapautta ja kaikkia vaihtoehtoisia tapoja ei testattu.

Potilasmonitori oletti fyysisesti läsnä olevan käyttäjän luotettavaksi, joten siihen pääsy tulisi estää asiattomilta henkilöiltä. Toinen vaihtoehto on olla säilyttämättä potilastietoja laitteessa. Standardit eivät ratkaise kaikkia turvallisuusongelmia, mutta ne tukevat määrittelemällä turvallisuudelle vähimmäistason. Silloin voimme luottaa tarvitsemamme lääkintälaitteen olevan riittävän turvallinen.

Avainsanat: lääkintälaitteet, sulautetut järjestelmät, kyberturvallisuus, kyberturvallisuusstan-

dardit, kyberturvallisuustestaus, Internet of Things

Abstract: Medical devices with information technology keep us alive if our body gives way. For example, smart defibrillators enable a nonprofessional to give effective first aid in case of a heart attack. Using information technology in medical devices bring possibilities but also threats. This study looks into the way standards and testing contribute to cybersecurity and controlling threats. First, there is a review into the literature and standards and then this knowledge is connected to practice by testing a patient monitor based on the literature.

The result was that the studied patient monitor is very open when used through its physical interface. For example, patient information was accessible and could be edited without signing in. There was practically no connection to be made through its telecommunications links. The monitor passed some of the requirements picked from the literature. Whether the monitor passed was unclear with a couple of the requirements as those gave developers some freedom and not all the possibilities were tested.

The patient monitor assumed a physically present user to be reliable so unauthorized people should be prevented accessing it. Another option would be to not keep patient information in the device. Standards won't solve all security problems but they support by defining minimum level of security. This way we can rely on the medical devices we need to be secure enough.

Keywords: medical devices, embedded computing, cyber security, cyber security standards, cyber security testing, Internet of Things

Termiluettelo

Kyberavaruus	“Kybermaailma on ihmisten, ohjelmistojen ja palveluiden vuorovaikutuksesta syntyvä monimutkainen ympäristö” joka toimii tietotekniikan ja tietoverkkojen päällä (*ISO/IEC 27032:2012* 2012, pykälä 4.21)
Kyberturvallisuus	“Kyberavaruuden tiedon luottamuksellisuuden, eheyden ja saatavuuden säilyttäminen” (*ISO/IEC 27032:2012* 2012, pykälä 4.20)
Lääkintälaite	Instrumentti, laitteisto, väline, ohjelmisto, materiaali tai muu laite tai tarvike, jota käytetään ihmisen sairauden tai vamman diagnosointiin, ehkäisyyn, hoitoon tai lievitykseen, anatomisen tai fysiologisen toiminnan korvaamiseen tai muunteluun taikka hedelmöittymisen säätelyyn.
ISO	International Organization for Standardization. Laajin kansainvälinen standardointiorganisaatio (*Kansainvälinen standardointi – Suomen standardoimisliitto SFS ry* 2017)
IEC	International Electrotechnical Commission. Kansainvälinen sähköalan standardointiorganisaatio, joka on tiukassa yhteistyössä ISO:n kanssa (*Kansainvälinen standardointi – Suomen standardoimisliitto SFS ry* 2017)
ITU	International Telecommunication Union. Kansainvälinen televiestintäliitto, joka on YK:n alaisuudessa ja pyrkii saamaan maailman tietoliikenteen osat yhteensopiviksi ja yhteentoimiviksi (*Kansainvälinen standardointi – Suomen standardoimisliitto SFS ry* 2017)
IoT	Internet of Things. Esineiden Internet on “verkosto, joka yhdistää tavallisia fyysisiä objekteja tunnistettavilla osoitteilla siten, että se tarjoaa älykkäitä palveluita.” (Ma 2011, s. 920)
DoS	Denial of Service. Palvelunesto, jolloin tietoon tai palveluun ei päästä käsiksi. Yksi tapa hyökätä tietojärjestelmää vastaan.

VPN	Virtual Private Network. Verkkoliikenne reititetään salattuna epäluotettavan verkon yli luotettuun verkkoon.
CRC	Cyclic Redundancy Check. Viestien oikeellisuuden tarkistusmenetelmä häiriöiden varalta.
OSI-malli	Verkkoliikenteen kerroksellisuuden kuvaus. Alimpana on fyysinen kerros, sen päällä ovat linkki-, verkko-, kuljetus-, istunto-, esitystapa-, ja sovelluskerros.

Kuviot

Sisältö

1 Johdanto

Tietotekniikkaa hyödynnetään terveydenhuollossa yhä enemmän (Zeadally, Isaac ja Baig 2016). Tietoteknisten lääkintälaitteiden käyttöönotolla voidaan automatisoida lääkärien ja hoitajien työtä (Arney ym. 2011, s. 2376), tehostaa olemassa olevia menetelmiä ja mahdollistaa uusia hoitomuotoja.

Konkreettisia esimerkkejä hyödyistä on mm. se, että potilaiden elintoimintojen seuraaminen lääkintälaitteilla vapauttaa hoitajat muihin tehtäviin. Toisenlaista tehostamista tuovat digitaaliset lämpömittarit, joilla lämpötilan saa mitattua tarkasti, ja lämpötilan oikein lukeminen helpottuu. Sydämentahdistin puolestaan hoitaa tavalla, joka ei olisi mahdollista ilman tietotekniikkaa. Uusien mahdollisuuksien myötä tulee myös uhkia, joten kyberturvallisuus on otettava huomioon.

1.1 Kyberturvallisuus

Kyberturvallisuuden teoreettisen tarkastelun helpottamiseksi tässä työssä käytetään ISO:n määritelmää, jonka mukaan kyberturvallisuus tarkoittaa “kyberavaruuden tiedon luottamuksellisuuden, eheyden ja saatavuuden säilymistä” (*ISO/IEC 27032:2012* 2012, pykälä 4.20). Kyberavaruus puolestaan on “ihmisten, ohjelmistojen ja palveluiden vuorovaikutuksesta syntyvä monimutkainen ympäristö”, joka toimii tietotekniikan ja tietoverkkojen päällä (*ISO/IEC 27032:2012* 2012, pykälä 4.21). Näin voidaan jaotella turvallisuutta pienempiin osakokonaisuuksiin: luottamuksellisuuteen, eheyteen ja saatavuuteen.

Tietotekniikan mukanaan tuomien uusien mahdollisuuksien lisäksi myös sen mukana tulevat uhat on otettava huomioon. Lääkintälaitteiden kyberturvallisuus on noussut mediassa ja tiedeyhteisössä ajankohtaiseksi aiheeksi (esim. Donnelly 2017; Lee 2016; Gayle ym. 2017). Yhä useampi terveydenhuollon laite on yhteydessä tietoverkkoihin ja muihin laitteisiin, mikä lisää mahdollisuuksien lisäksi kyberturvallisuusuhkia (Arney ym. 2011). Yhteydet esimerkiksi seurantalaitteen ja lääkeannostelijan välillä mahdollistavat lääkkeen annostelun tarpeen mukaan, mutta tietoliikenne avaa myös ulkopuolisille reittejä vaikuttaa laitteiden toimintaan.

Kyberturvallisuuteen panostamiselle on tarvetta, sillä skyberavaruudelta suojaamaton laite uhkaa potilaan turvallisuutta siinä missä räjähdysherkkä akku: esimerkiksi sydämentahdistimen toiminnan pahantahtoisen muuttamisen seuraukset voivat olla vakavat. Halperin, Heydt-Benjamin, Ransford ym. (2008) saivat koeoloissa rytmihäiriöiden hoitoon käytettävän sydämentahdistimen kokeilemaan sähköiskun antamista. Näiden komentojen antaminen käytössä olevalle tahdistimelle antaisi potilaan sydämelle sähköiskuja. He onnistuivat todentamaan tämän heikkouden toistamalla komentoja, joita tahdistimen ohjelmointilaite lähetti sähköisku-toimintoa testattaessa. Sydämentahdistinten ja muiden tietoteknisten lääkintälaitteiden yleistyessä niiden kyberturvallisuus nousee tärkeämpään asemaan (*Content of Premarket Submissions for Management of Cybersecurity in Medical Devices* 2014).

1.2 Standardit

Standardit ovat yksi tapa tuoda turvallisuutta laitteisiin. Standardien tavoitteina on parantaa tuotteita, laskea kustannuksia ja edistää kommunikaatiota (Kajava ym. 2006, s. 2091). Turvallisuusstandardien ja -määräysten ansiosta jokaisen lääkintälaitteen tilaajan ei tarvitse määritellä haluamaansa turvallisuustasoa alusta asti, sillä perusvaatimukset täyttyvät, jos laite on saanut myyntiluvan. Jotta lääkintälaiteita voidaan myydä, on niiden täytettävä niitä koskevat säädökset ja sitovat standardit markkinamaassa. Näissä säädöksissä keskitytään laitteen tehollisuuteen ja käyttöturvallisuuteen (Rostami, Juels ja Koushanfar 2013; Halperin, Heydt-Benjamin, Fu ym. 2008). Laitteiden vaaditaan siis antavan tehokasta hoitoa, jotta niiden käytöstä on hyötyä. Lisäksi käytöstä ei saa olla suhteetonta haittaa potilaalle verrattuna hyötyyn.

Lääkintälaitteiden kyberturvallisuudelle on standardeja, joiden avulla saavutetaan jonkinlainen minimitaso. Suomen kannalta tärkeimmät standardit ovat Euroopan Unionin hyväksymät ISO-standardit. Yhdysvalloissa FDA:lla on omat standardinsa, mutta ne eivät koske Eurooppaa. Näiden standardien noudattaminen ja kyberturvallisuusominaisuuksien testaaminen on tärkeää, jotta voidaan olla varmempia turvallisuudesta. Tiedetään, että käytetään yleisesti toimiviksi todettuja, standardeihin hyväksyttyjä periaatteita ja testaamalla varmistetaan, että toteutuskin on onnistunut.

Lääkintälaitteiden kyberturvallisuudesta on kertynyt tietoa ja sitä on kirjattu standardeihin. Tiedon käyttöönotossa testaaminen on yksi tapa varmentaa että kaikki toimii niin kuin pitää. Mahdollisimman konkreettiset testit pakottavat määrittelemään vaatimukset tarkasti ja siten väärinymmärrysten määrä vähenee.

1.3 Tutkimuskysymys

Tämän tutkimuksen tavoitteena on tuottaa standardeihin nojaava viitekehys lääkintälaitteiden kyberturvallisuuden testaamiselle. Ensin avataan lääkintälaitteiden kyberturvallisuuden nykytilaa ja siihen luotuja standardeja. Sitten käydään läpi standardien testaustapoja ja konkretisoidaan yhden lääkintälaitteen testaamisella.

Tutkielman rakenne on seuraava: Luvussa 2 käydään läpi menetelmät, joita käytettiin kirjallisuuden keräämiseen, standardien analysointiin ja laitteiden testaamiseen. Luvussa 3 perehdytään kyberturvallisuuden määritelmiin, uhkiin ja suojauskeinoihin. Lääkintälaitteiden erityispiirteitä ja ominaisuuksia käydään läpi kappaleessa 4. Tutkielman empiirisessä osuudessa, luvussa 7, testataan esimerkinomaisesti erään lääkintälaitteen kyberturvallisuutta suhteessa standardeihin ja suosituksiin. Viimeisenä ovat johtopäätökset luvussa 9.

2 Tutkimusmenetelmät

Tässä kappaleessa käydään läpi tutkielman tutkimusmenetelmiä. Menetelmien läpikäynti tukee tutkimuksen perusteellisuutta ja toistettavuutta. Tutkimuksen laatuun ja hyödyllisyyteen vaikuttaa tutkijan tietoisuus tutkimuksen vaiheista ja menetelmistä (Jenkins 1985, s. 97).

2.1 Metodi

Tässä tutkielmassa käytetään konstruktiivista tutkimusotetta. Konstruktiivisessa tutkimuksessa ratkaistaan ongelma luomalla uusi konstruktio (Kasanen, Lukka ja Siitonen 1993). Konstruktio on määritelty hyvin laveasti. Kaikki mitä ihmiset tuotavat ovat konstruktioita, kuten mallit, toimintatavat, kuvat, laitteet ja lääkkeet (Kasanen, Lukka ja Siitonen 1993). Konstruktiivinen tutkimus on hyvin lähellä design science -tutkimusta ja sen voikin nähdä design science -tutkimuksen alatyyppinä (Piirainen ja Gonzalez 2013). Nämä tutkimustavat ovat kuitenkin lähtöisin eri tieteenaloilta: konstruktiivinen liiketaloustieteestä ja design science taas tietojärjestelmätieteestä ja ne käyttävät eri termejä (Piirainen ja Gonzalez 2013).

2.2 Kirjallisuuskatsaus

Kirjallisuus kerättiin lähinnä hakusanoilla hakemalla eri tietokannoista. Käytettiin myös vähäisessä määrin lumipallohakua, jota suositellaan pelkän hakusanahaun tueksi (Runeson ja Höst 2009, s.15). Siinä käydään valittujen artikkeleiden lähteitä läpi ja jos jo poimitun artikkelin lähteistä löytyi nimen perusteella aiheeseen tiukasti liittyviä artikkeleita, nekin tarkistettiin (Kitchenham ja Brereton 2013, s. 2052). Puhtaasti hakusanahakua käytettäessä on riski, että oleelliset julkaisut jäävät huomiotta, jos niissä on käytetty eri termiä kuin hakusanoissa. Siksi hakustrategiaa tehdessä tulee ottaa huomioon mm. synonyymit (Runeson ja Höst 2009, s. 14). Pelkkää lumipallohakua käytettäessä taas uhkana on, että saadaan liikaa saman kirjoittajan teoksia suhteessa muiden töihin (Jalali ja Wohlin 2012, s. 36).

Lääkintälaitteiden kyberturvallisuudesta kertova kirjallisuus kerättiin avainsanahaulla tietokannoista IEEE:n, ACM:n, Scopuksen ja Proquestin tietokannoista. Tärkein hakutermiyhdistelmä

oli “medical device security”. Näillä sanoilla löytyi hakutuloksia eri tietokannoista seuraavasti: Scopus 2 544 kpl, Proquest 1 293 kpl, ACM 69 997 kpl, IEEE 968 kpl. ACM:n luokittelujärjestelmän lähimmäksi osunut termi “Embedded systems security” tuotti myös paljon tuloksia. Kun hakua tarkensi sanalla “medical”, saatiin tarkemmin aiheeseen liittyviä tuloksia. Näissä artikkeleissa oli suhteessa enemmän lääkinnällisiin implantteihin liittyviä artikkeleita.

Avainsanoilla löydetyistä artikkeleista karsittiin pois ne, jotka eivät liittyneet kyberturvallisuuteen tai lääkintälaitteisiin. Lisäksi hylättiin lähteet, jotka keskittyivät lääkinnällisiin ohjelmistoihin eivätkä erikoistuneisiin fyysisen laitteen sisältäviin kokonaisuuksiin. Myös *in vitro* -diagnostiikkaan tarkoitetut laitteet jätettiin pois. *In vitro* tarkoittaa sananmukaisesti *lasissa*, eli tutkitaan näytteitä potilaan ulkopuolella, monesti lasiputkessa (*In Vivo | Definition by Merriam-Webster* 2017). Esimerkiksi verinäytteet tutkitaan *in vitro*. Vastakohtana on *in vivo*, eli *elävässä*, jolloin tutkimuksen kohde on tutkimuksen ajan elävä ja ehjä (*In Vivo | Definition by Merriam-Webster* 2017). Esimerkiksi syke mitataan *in vivo*.

Hakusanoilla “authentication electricity body” haettiin tietoa kehoon laitettavien laitteiden sähköisestä autentikoinnista IEEE:n ja ACM:n tietokannoista. Kirjallisuutta turvallisuusstandardien käytöstä ja hyödyllisyydestä haettiin hakutermillä “information security standard” käyttäen IEEE:n (21 kpl), ACM:n (9 kpl) ja Springerin (209 kpl) tietokantoja. Springerin tuloksia rajattiin vuoden 2010 jälkeen julkaistuihin, jolloin tuloksia oli vain 142. Kun hakuehdoksi vaihdettiin “cyber security standard” tai “cybersecurity standard”, IEEE:ltä löytyi 18 julkaisua, ACM:ltä vain yksi julkaisu, Springeriltä 76 julkaisua.

Tutkimusmetodeista haettiin Scopuksen kirjastosta julkaisuja, joiden otsikossa oli“research method”. Tämä tuotti yli 3 000 osumaa, joten hakua rajattiin siten, että otsikossa, abstraktissa tai avainsanoissa olisi “information technology”. Tuloksia oli enää 27. Viestinnän turvallisuuden metodeista ja kontrolleista haettiin IEEE:n tietokannoista hakutermillä “Communication System Security methods OR tools”. Tällä tavalla saatiin 558 tulosta.

Turvallisuuden testauksesta etsittiin julkaisuja hakusanalla “Security testing”. Tuloksia tuli valtava määrä: IEEE 20 329 kpl, ACM 73 372. Tuloksia rajattiin Springerin julkaisukirjastossa rajaamalla alaksi tietotekniikka, jolloin saatiin 82 299 julkaisua. ProQuestillä “Security testing” osui 118 376:een julkaisuun. Kun rajattiin vertaisarvioituihin, määrä pieneni 7 916. Edelleen

rajaamalla niihin joiden koko teksti oli saatavilla saatiin määrä pienenemään 1 293:een.

2.3 Standardit

Tässä työssä käytettiin seuraavia standardeja ja teknisiä raportteja:

- ISO/IEC 15408-1:2009 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model
- ISO/IEC 15408-2:2008 Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components
- ISO/IEC 15408-3:2008 Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components
- IEC/TR 80001-2-2:2012 Application of risk management for IT-networks incorporating medical devices – Part 2-2: Guidance for the communication of medical device security needs, risks and controls
- IEC/TR 80001-2-3:2012 Application of risk management for IT-networks incorporating medical devices – Part 2-3: Guidance for wireless networks

Näihin päädyttiin, koska arviointikriteerien uskottiin olevan helposti muunnettavissa toteutettaviksi testeiksi. Lisäksi Anita Finnegan ja Fergal McCaffery (2015) käyttivät IEC/TR 80001-2-2 ja IEC/TR 80001-2-3 -teknisiä raportteja ja heidän työstään kävi ilmi, että raporteissa on melko konkreettisia vaatimuksia.

Tietoturvallisuuden hallintajärjestelmän standardiperhe ISO/IEC 27000 jätettiin käsittelemättä, vaikka se on erittäin keskeinen tieto- ja kyberturvallisuudessa. Kyseiset standardit jätettiin pois, sillä ne eivät keskity teknisiin vaatimuksiin vaan enemmän organisaation prosesseihin, ja siten ovat tämän työn ulkopuolella. Organisaatioiden prosessien, henkilöstön ja fyysisten turvatoimien tärkeyttä ei kuitenkaan voida kiistää. Teknisiin turvallisuusvaatimuksiin keskittyvä *ISO/IEC 15408-1:2009* (2009, s. vi) mainitsee kyseisen standardin, mutta rajaa sen aiheensa ulkopuolelle. ISO/IEC 27002 -standardista on tehty lääkintälaitteille oma standardi ISO 27799:2016. Nämä standardit on jätetty käsittelemättä, koska ne ovat lähinnä suosituksia, eikä niiden noudattamista voida välttämättä tarkistaa (Calder 2008, s. 19).

2.4 Testaus

Testauksessa käytettiin IEC/TR 80001-2-2:n listaamia turvavaatimuksia. Kaikkia ei kuitenkaan testattu, vaan testattavat vaatimukset valittiin laitteen ominaisuuksien ja testausvalmiuksien perusteella. Esimerkiksi laitteen sisäisiin järjestelmiin ei ollut pääsyä, joten erilaisten lokien olemassaoloa ei voitu varmentaa. Tutkittavalla monitorilla on joitain tietoliikenneyhteyksiä. Siinä on Ethernet-portti, tulostimelle tarkoitettu sarjaportti ja sarjaporttimainen liitäntä, jonka kytkennät kuitenkin eroavat sarjaportista. Tätä erikoista liitäntää kutsutaan ohjekirjoissa "Coding element"-nimellä, joka suomennetaan tässä tutkielmassa ohjelmointikytkennäksi.

3 Kyberturvallisuus

Kyberturvallisuudelle löytyy monta, osittain ristiriitaista määritelmää. Aluksi katsotaan kyber-etuliitteen käyttöä, sitten kyberavaruuden ja tietoturvallisuuden määritelmiä. Lopuksi käydään läpi joitain viranomaisten näkemyksiä kyberturvallisuudesta.

3.1 Kyberturvallisuuden määritelmistä

Mitä 'kyber' on? Kyber-etuliitteen juuret ovat kreikassa, kybernētēs-sanassa, joka tarkoittaa hallintaa, ohjaamista (*Cyber- Definition by Merriam-Webster* 2017; *Cybernetics- Definition by Merriam-Webster* 2017). Kybernetiikka-sana sidottiin tietotekniikkaan Norbet Weinerin kirjassa "Cybernetics or Control and Communication in the Animal and the Machine" vuonna 1948 (*Definition of Cybersecurity* 2016). Kyber-etuliite on elänyt villiä elämää ja on liittynyt lukuisille tieteen ja taiteen aloille. Esimerkiksi William Gidson antoi romaanissaan Necromancer kuvauksen futuristisesta kyberavaruudesta, jossa kaikki on liittyneenä kaikkeen, ja 60-luvulla yhden tyyppinen tanssi oli nimeltään kyberavaruus (*Definition of Cybersecurity* 2016, s. 10). Kyber-etuliitettä on käytetty varsin laajasti ja kyberturvallisuuden määritteleminen on lähes yhtä vaikeaa kuin turvallisuuden määritteleminen ilman etuliitettä (*Definition of Cybersecurity* 2016, s. 10).

Määritelmiä kyberturvallisuudelle on kerätty standardointilaitoksilta, kuten International Organization for Standardization (ISO), ja valtioilta, esimerkiksi niiden kyberturvallisuustrategioista. Monet näistä strategioista eivät määrittele kyberturvallisuutta ja annetut määritelmät eivät ole yhdenmukaisia (Luiijf ym. 2013). *Definition of Cybersecurity* (2016, s. 24 - 25) nostaa esille, että kyberturvallisuuden standardoinnissa on päällekkäisyyksiä ja aukkoja. Sen mukaan esimerkiksi kyberavaruuden määrittely on hajanaista ja turvallisuuden arviointiin ei ole työkaluja.

Kyberturvallisuus voidaan ajatella kyberavaruuden turvallisuutena. Mitä on sitten kyberavaruus? *CNNSI No. 4009* (2010) kuvailee kyberavaruuden osana tietoympäristöä, "koostuen toisistaan riippuvista tietojärjestelmien infrastruktuureista, mukaan lukien Internet, televiestintäverkot, tietokonejärjestelmät ja sulautetut prosessorit ja kontrollerit". Tämän mukaan kybe-

ravaruus olisi verkosto, joka sisältää kaiken tietoliikenteen. Suomen kyberturvallisuusstrategia (2013) pitää kybertoimintaympäristöä, joka vastaa kyberavaruutta, myös tietoa käsittelevänä verkostona, mutta liittää siihen fyysisen ja virtuaalisen infrastruktuurin lisäksi palvelut ja kutsuu kyberavaruutta verkoston sijaan ympäristöksi. ISO:n kyberturvallisuusohjeistuksen mukaan kyberavaruus on tietotekniikan ja tietoverkkojen päällä toimiva "ihmisten, ohjelmistojen ja palveluiden vuorovaikutuksesta syntyvä monimutkainen ympäristö" (*ISO/IEC 27032:2012* 2012, pykälä 4.21). Tämä määritelmä lisää kyberavaruuteen ihmiset.

Kyberturvallisuudelle läheinen käsite on tietoturvallisuus, ja jotkin viranomaiset määrittelevät kyberturvallisuuden tietoturvallisuuden avulla. Tiedon turvallisuudesta on yleisesti käytössä oleva malli, lyhennettynä CIA: luottamuksellisuus (Confidentiality), eheys (Integrity) ja saavutettavuus (Availability) (Whitman ja Mattord 2011, s. 8). Luottamuksellisuudella tarkoitetaan, että käyttäjät, joille ei ole annettu oikeutta tietoon, eivät saa sitä käsiinsä (Weippl, Holzinger ja Tjoa 2006). Eheydellä tarkoitetaan, että tietoa voivat muuttaa vain siihen oikeutetut henkilöt ja ohjelmat (Weippl, Holzinger ja Tjoa 2006). Tiedon saavutettavuus on kolmas tavoite, sillä luottamuksellinen ja eheä tieto, johon ei päästä käsiksi tarvittaessa, on hyödytöntä.

Monet tahot määrittelevät tietoturvallisuuden ja kyberturvallisuuden CIA-kolminaisuuden pohjalta. Esimerkiksi ISO määrittelee tietoturvallisuuden standardissaan tiedon CIA:na, lisäten, että myös "autenttisuus, tilivelvollisuus, kiistämättömyys ja luotettavuus voivat olla osallisena" (*ISO/IEC 27000:2016* 2016, pykälä 2.33). *Definition of Cybersecurity* (2016) -katsaus jaottelee kyberturvallisuuden määritelmät myös sen mukaan, mainitaanko CIA-kolminaisuus. Muitakin näkemyksiä tieto- ja kyberturvallisuudesta on, mutta CIA on yleisessä käytössä oleva malli.

ISO:n kyberturvallisuusohjeistus *ISO/IEC 27032:2012* (2012, pykälä 4.19 ja 4.20) on määritellyt kyberturvallisuuden kahdessa osassa englannin kielen sanojen 'security' ja 'safety' mukaan. Molemmat kääntyvät suomeksi 'turvallisuus', mutta niillä on vivahde-ero. Kyberturvallisuus, 'cybersecurity', on määritelty kyberavaruuden tietoturvallisuutena, eli se on "kyberavaruuden tiedon luottamuksellisuuden, eheyden ja saatavuuden säilyttäminen" (*ISO/IEC 27032:2012* 2012, pykälä 4.20). Edelliseen määritelmään liitetyn kommentin mukaan kyberturvallisuuteen voidaan katsoa kuuluvan myös "autenttisuus, tilivelvollisuus, kiistämättömyys ja luotettavuus".

Sen sijaan kyberturva (’cybersafety’), määritellään tilana, jossa ollaan suojassa kaikilta eihalutuilta seurauksilta, jotka johtuvat kyberavaruuden tapahtumista. Tämä sisältää mm. fyysiset, sosiaaliset, hengelliset ja ammatilliset seuraukset. Tämä määritelmä on ihmiskeskeinen: ihmiset ovat turvassa kaikelta ikävältä, mitä kyberavaruudesta voi seurata. Voiko tätä tilaa, kyberturvaa, koskaan saavuttaa? Kyberkiusaaminen nousee ihmisten mieleen, kun puhutaan kyberturvallisuudesta (Martin ja Rice 2011). Ihmiset kuuluvat ISO:n kuvaan kyberavaruudesta (*ISO/IEC 27032:2012* 2012, pykälä 4.21), joten jos ihmiset voivat ympäristössä keskustella vapaasti ja esimerkiksi juoruilemalla aiheuttaa toiselle sosiaalista haittaa, eivät ihmiset ole kyberturvassa.

Viranomaiset ovat ristiriidassa jo määritelmiensä ytimessä. Jotkut määrittelevät kyberturvallisuuden tilana, osa taas työvälineenä ja kolmannet puolustuskykynä. Suomen kyberturvallisuusstrategiassa kyberturvallisuus märitellään tavoitetilaksi, jossa kybermaailma on luotettava: sekä sen toiminnan turvallisuuteen että jatkuvuuteen voidaan luottaa (Suomen kyberturvallisuusstrategia 2013). Toisaalta kansainvälisen televiestintäliitto ITU:n näkemyksen mukaan kyberturvallisuus ei ole tavoite, vaan välineistö kyberympäristön ja sitä käyttävien järjestöjen ja henkilöiden resurssien turvaamiseksi (*Recommendation ITU-T X.1205* 2008, s. 2, pykälä 3.2.5). ITU:n suosituksen mukaan tämä välineistö pitää sisällään turvallisuuskäsitteet, ohjeistukset, työkalut ja teknologiat, joilla pidetään järjestöjen ja käyttäjien laitteet, henkilökunta ja palvelut sekä tiedot turvassa. *CNNSI No. 4009* (2010) ja *NIST Special Publication 800-39* (2011) esittävät kyberturvallisuuden puolustuskykynä hyökkäyksiä vastaan. *NIST Special Publication 800-39* (2011) määrittelee, että kyberturvallisuus on “kyky suojella tai puolustaa kyberavaruuden käyttöä kyberhyökkäyksiltä.”

Nämä vaihtoehtoisista näkökulmista kyberturvallisuus tavoitetilana tai työvälineenä - määritelmät näkyvät myös viranomaismääritelmien ulkopuolella, englannin kielessä. *cyber -, comb. form : Oxford English Dictionary* (2017) määrittelee kyberturvallisuuden olevan ”tietokonejärjestelmiin ja Internetiin liittyvä turvallisuus”, ja turvallisuus on huolettomuutta, eli tavoitetila. *Cybersecurity | Definition by Merriam-Webster* (2017) puolestaan esittää, että kyberturvallisuutta ovat “toimenpiteet, joilla suojellaan tietokonetta tai tietokonejärjestelmää (kuten Internetissä) luvatonta pääsyä ja hyökkäystä vastaan”. Kyberturvallisuutta ja tietoturvallisuutta käytetään monesti synonyymeinä, mutta Solms ja Niekerk (2013) erot-

televat näitä termejä. Heidän mallissaan turvallisuudella on kolme osa-aluetta ja kerrosta. Osa-alueita ovat uhat, haavoittuvuudet ja resurssit. Turvallisuuden kerrokset eroavat siinä, mitkä ovat turvattavia resursseja ja minkä haavoittuvuudet aiheuttavat uhkia. Kerrokset ovat informaatioteknologian turvallisuus, tietoturvallisuus ja kyberturvallisuus. Alemman kerroksen haavoittuvuudet uhkaavat korkeamman kerroksen resursseja, eli aukko teknologiassa vaarantaa tietoturvallisuuden, mikä vuorostaan avaa reittejä kyberturvallisuuden uhkaamiseen.

Solms ja Niekerk (2013) rajaavat, että tietoturvallisuudella tarkoitetaan nimenomaan tiedon turvassa pysymistä. Tietoturvallisuuden uhkia aiheuttavat haavoittuvuudet tietoviestintäteknologioissa, sillä tieto ja sen käsittely rakentuvat teknologian päälle. Kyberturvallisuus puolestaan nostaa suojeltavat resurssit seuraavalle tasolle: ihmiset. Kyberturvallisuus on heille ihmisten ja ihmisten tavoitteiden suojelemista kybermaailman uhilta (Solms ja Niekerk 2013). Resurssien uhat mahdollistaa mallin edellinen kerros: tiedon käsittelyssä on haavoittuvuuksia.

Solms ja Niekerk (2013) nostavat tietoturvallisuuden ja kyberturvallisuuden erosta esimerkiksi älykodinlaitteiden haltuunoton: kahvinkeittimen tai hälytysjärjestelmän kytkeminen pois päältä ei välttämättä vaadi hyökkäyksen kohteen tietojen vuotamista tai muuttamista, joten ne eivät aina kuulu tietoturvallisuuden piiriin. Kohteen tavoitteet saada tuoretta kahvia ja pitää kotinsa turvallisena eivät täyty, joten älykodin kyberturvallisuus on huonolla tolalla, vaikka tietoturvassa ei olisi moitittavaa. Lääkintälaitteiden ja hoivalaitteiden kohdalla tämä voidaan tulkita siten, että potilastietojen yksityisyys kuuluu nimenomaan tietoturvallisuuden piiriin ja laitteiden fyysinen toiminta enemmän kyberturvallisuuteen. Tässä tutkielmassa tietojen turvassa pysymistä käsitellään osana kyberturvallisuutta, sillä ne ovat kytkeytyneet toisiinsa ja tietoturvallisuuden heikkous heikentää kyberturvallisuuttakin.

Kyberavaruudelle ja -turvallisuudelle ei ole siis kaikille yhteistä määritelmää. Näkemykset eroavat kohteiltaan ja laajuudeltaan. Kyberavaruus on joillekin tietoverkostot, jotkut taas sisällyttävät kaiken, mikä on tekemisissä tietoverkkojen kanssa, osaksi kyberavaruutta. Kyberturvallisuus on joillekin turvaamiseen käytettävät työkalut, joillekin käytännössä sama kuin tietoturvallisuus: tiedon luottamuksellisuus, eheys ja saavutettavuus. Joillekin kyberturvallisuus on tila, jossa tietoverkoissa oleva toiminta ei aiheuta haittaa kellekään tai millekään. Laajimmat määritelmät kattavat kaiken, mitä kukaan mieltää kyberturvallisuudeksi, mutta tiukempi määritelmä voisi olla hyödyllisempi arvioitaessa jonkin laitteen tai verkon kyberturvallisuutta.

vallisuuden tilaa.

3.2 Uhat

Uhkina ovat tahallinen vahingonteko, tahattomat toimet ja luonnollisesti ilmaantuvat uhat. Uutisotsikoihin on noussut tapauksia, joissa sairaaloiden tietojärjestelmät on tahallisesti salattu, jolloin elintärkeät tiedot ovat lääkäreiden ja hoitajien saavuttamattomissa (Donnelly 2017; Lee 2016; Gayle ym. 2017). Salattuaan järjestelmät rikolliset vaativat rahaa tietojen vapauttamista vastaan. Rikollisen ja tahallisen toiminnan lisäksi järjestelmien toimintaa voidaan haitata tahattomilla toimilla. Tällainen tahattomuus esti pääsyn Jyväskylän terveydenhuollon potilastietojärjestelmiin, kun palomuuri säädettiin väärin (Raitio 2015). ”Luonnollisesti ilmaantuvat” uhat on otettu huomioon esimerkiksi lääkintälaitteiden verkottumisen turvaamisessa (Taylor, Venkatasubramanian ja Shue 2014). Luonnollisesti ilmaantuvilla uhilla tarkoitetaan kaikkea, mitä kukaan ihminen ei aiheuta tahallaan, esimerkiksi sähkökatko tai viestejä muuttava kohina. Luonnollisesti ilmaantuvien uhkien lisäksi tulee pystyä puolustautumaan tahallisia hyökkäyksiäkin vastaan.

3.2.1 Ihmiset

Ihmiset ovat monesti uhka kyberturvallisuudelle (Renaud ja Goucher 2014). Erityisesti sisäpiiriläisten toimet ovat kyberturvallisuuden kannalta oleellisia. Greitzer ym. (2008) määrittelevät sisäpiiriläisiksi luotetut henkilöt, esimerkiksi yrityksen työntekijät ja aliurakoitsijat, joilla on tai on ollut pääsy yritysten järjestelmiin. Heidän mukaansa sisäpiiriläisten toiminta on kyberturvallisuutta uhkaavaa, kun työntekijä ei noudata ohjeistuksia, johtui tottelemattomuus sitten pahantahtoisuudesta tai välinpitämättömyydestä. Kyberturvallisuuden jääminen huomiotta voi kummuta myös positiivisesta asiasta. Williams (2008) katsovat tutkimuksensa pohjalta, että terveydenhuollon ammattilaiset ovat taipuvaisia luottamaan henkilökuntaan ja ohjelmistoihin. Tähän luottamukseen nojaten kyberturvallisuustoimet saatetaan jättää kehittämättä ja panematta täytäntöön.

Greitzer ym. (2008) näkevät kouluttamisen olevan avainasemassa: sekä työntekijöiden koulutus että sisäpiiriläisuhkien tunnistamisen opettaminen parantavat kyberturvallisuutta. Sisä-

piiriläisten kyberturvallisuutta uhkaavaa toimintaa voidaan vähentää tiedon jakamisella ja selkeyttämisellä. Esimerkiksi vastuiden epäselvyys ja tietämättömyys riskeistä edesauttaa turvallisuuskäytäntöjen laiminlyöntiä (Williams 2008) ja *IEC/TR 80001-2-2:2012* (2012, pykälä 5.16) nostaa esille turvallisuusohjeiden antamisen käyttäjille ja järjestelmänvalvojille.

Käyttäjät turvallisuuden vihollisina on teknologiakeskeinen näkökulma, jonka myötä kyberturvallisuuden kehityksessä on perinteisesti luotettu turvallisuustekniikan kehitykseen (Laszka, Felegyhazi ja Buttyan 2014, s. 23:1). Käyttäjät tuskin pyrkivät heikentämään kyberturvallisuutta, mutta jotkin turvamenettelyt koetaan liian hankaliksi käyttää ja käyttäjät eivät ole motivoituneita niitä noudattamaan. Tämä johtunee siitä, että käyttäjät eivät tiedosta kyberturvallisuuden tärkeyttä ja turvallisuusasiantuntijat eivät ota huomioon käyttäjien toimia ja tarpeita (Adams ja Sasse 1999, s. 43). Pitkien salasanojen käyttämisen ja jatkuvan vaihtamisen vaatiminen ovat idealtaan kyberturvallisia. Huonon käytettävyyden vuoksi hankalien salasanojen käyttöä kuitenkin kierretään parhaan mukaan, jotta käyttäjän muu toiminta ei kärsisi, minkä myötä turvalliset toimet vesittyvät (Adams ja Sasse 1999, s. 44). Käyttäjien pelottelu varoituksilla on toinen lähestymistapa, mutta liian suuri määrä vääriä hälytyksiä johtaa tottumiseen ja käyttäjä vain etenee rutiininomaisesti varoitusten ohitse (Sasse 2015).

Jotta käyttäjät toimisivat turvallisesti, tulee turvatoimien olla käytettäviä ja niitä tehdessä ja arvioitaessa on otettava huomioon käyttäjät ja heidän tehtävänsä. Tätä ajatusta tukevat Krens, Spruit ja Urbanus (2013), jotka ehdottavat holistisempaa näkemystä kyberturvallisuuteen terveydenhuollossa. Siinä lähtökohtana on hoidon toimiminen ja potilaiden turvallisuus. Lähtökohdan muuttaminen käyttöaluelähtöiseksi voisi auttaa terveydenhuollon ammattilaisia käyttämään turvallisia laitteita, ohjelmia ja menetelmiä. Krens, Spruit ja Urbanus (2013) nostavat turvallisuuden toimivuuden tutkimiseen kolme näkökulmaa: lakien ja standardien noudattaminen, tehokkuusmittarit ja loppukäyttäjän mielikuva. Näiden lisäksi he kehittivät terveydenhuollossa käytössä olevan arviointityökalun, Manchester Patient Safety Framework (MasPSaF), pohjalta uuden, tietoturvaan keskittyvän arvioinnin nimeltään Information Security Employee's Evaluation (ISEE). Kokeiluissa havaittiin, että arviointityöpajassa terveydenhuollon ammattilaiset arvioivat tietoturvallisuutta johdonmukaisesti, huomasivat ongelmakohtia ja keksivät niihin ratkaisuja. Tällainen käyttäjien ottaminen mukaan ongelmanratkaisuun edistää päätöksien noudattamista, jolloin turvallisuuskin paranisi

tästä näkökulmasta toimimalla (Kirlappos, Beautement ja Sasse 2013).

3.2.2 Kerrokset

Tietotekniikka rakentuu monesti kerroksiksi. Alimpana ovat fyysiset laitteet ja yhteydet, sen päälle on rakennettu tiedon käsittely prosessoreissa ja siirtäminen kaapeleissa. Jokainen kerros abstraktoi tietokoneiden ja -verkkojen toimintaa. Esimerkiksi käyttöjärjestelmät piilottavat fyysiset laitteet niin, että ohjelmistojen tekijöiden ei tarvitse tehdä tuotteestaan omia versioita esimerkiksi jokaiselle prosessorityypille erikseen. Puolestaan Internetiä käytettäessä ihmisystävälliset nimet, kuten google.com piilottavat sivustojen servereiden IP-osoitteet (esim. 8.8.8.8).

Kerrokset monesti luottavat alempien kerrosten toimivan oikein, jolloin voi avautua reittejä järjestelmien kimppuun. “Linnan muurin ali kaivautuminen” oli toimiva strategia keskiajan linnojen vahvoja puolustuksia vastaan ja se vaikuttaa tehokkaalta lähestymistavalta kyberrikollisille (Wilson ja Kiy 2014, s.117). Esimerkiksi jos haittaohjelma väärentää käyttöjärjestelmän kutsuja tai niiden dataa, ovat sovelluksen keinot turvata tilanne vähissä (Wang ym. 2009, s. 545). Loppujen lopuksi laitteiston turvallisuus on perimmäinen vaatimus, eikä sekään ole itsestäänselvyys. Esimerkiksi muistiosoitteet voivat häiritä toisiaan, jolloin tallennettu bitti muuttuu toiseksi viereisen muistikohdan kirjoittamisen vuoksi (Kim ym. 2014). Tätä ilmiötä hyödyntäviä hyökkäyksiä kutsutaan RowHammer-hyökkäyksiksi (Burleson, Mutlu ja Tiwari 2016). Niillä on onnistuttu ottamaan lisää oikeuksia Linux-järjestelmässä, jonka myötä saa vapaat kädet tehdä järjestelmälle mitä haluaa (Seaborn 2015).

3.3 Uhkien torjunta

Vaikkakin turvallisuus saavutetaan ITU:n mukaan prosessilla, eikä irrallisilla moduuleilla (*Recommendation ITU-T X.1205* 2008, s. 6), osien erottaminen kokonaisuudesta helpottaa asian analysointia. *ISO/IEC 15408-1:2009* (2009) nimittää yksittäisiä turvallisuusmoduuleita vastatoimiksi. Vastatoimien analysoinnissa on kyseisessä standardissa kaksi osaa: vastatoimen riittävyys ja oikeellisuus (*ISO/IEC 15408-1:2009* 2009, pykälä 6.2). Riittävyydellä tarkoitetaan ideaalin vastatoimen tehokkuutta: vähentäisikö se torjuttavaa riskiä. Oikeellisuus koskee

toteutusta: tekeekö tutkittava asia sen, mitä siltä edellytetään.

Kokonaista järjestelmää voidaan suojata koventamalla. Koventamisen päämääränä on vähentää hyökkäysvektorien määrä minimiin (*IEC/TR 80001-2-2:2012* 2012, pykälä 5.15). Hyökkäysvektori on hyökkäyksen reitti kohteeseen, esimerkiksi sähköpostin liitetiedosto tai Bluetooth-yhteys (Hansman ja Hunt 2005, s. 37). Joskus jaotellaan hienosyisemmin niin, että hyökkäyspinta on rajapinta, jonka kautta hyökkäys tulee, ja hyökkäysvektori tarkempi kuvaus reitistä hyökkäyspinnalta kohteeseen (Serrano ym. 2013, s. 280). Tässä työssä hyökkäysvektorilla tarkoitetaan kuitenkin laajempaa rajapintaa.

Turvallisuuden ja muiden ominaisuuksien välillä on jännite. Kätevyyttä ja käytettävyyttä uhrataan turvallisuuden vuoksi ja toisinpäin. Kybertuvallisuutta heikennetään mm. pilvipalveluja käytettäessä kätevyyden nimissä ja lääkintälaiteimplanttien tarjoaman itsenäisyyden vuoksi (Altawy ja Youssef 2016, s. 959 ja 964)

3.3.1 Luottamuksellisuus

Luottamuksellisuudella tarkoitetaan, että laitetta, ohjelmaa tai niiden tietoja voivat käyttää vain ihmiset, laitteet ja ohjelmat, joilla on siihen oikeus. Jos luottamuksellisuus ei ole kunnossa, yksityiset tiedot voivat päätyä vääriin käsiin ja joku ulkopuolinen voi säätää älykodin lämpötilaa. Pyrkimyksenä on siis pitää ulkopuoliset ulkopuolisina. Tämän varmistamiseksi on erilaisia keinoja, joista nostetaan esiin palomuurin, autentikoinnin, salauksen, ja virtual private networkin eli VPN:n.

Palomuurit Palomuurien tarkoituksena on olla verkon rajalla ja päästää läpi vain sallitut paketit ja jättää välittämättä sääntöjen vastaiset viestit. Sallittu viesti on reitti järjestelmään eli hyökkäysvektori. Sallittujen viestien määrän minimointi ja muidenkin vaikutusmahdollisuuksien karsiminen kuuluu koventamiseen.

Salaus Salauksen avulla estetään salakuuntelu. Ilman avainta ei salattua tietoa voida hyödyntää. Tieto voi olla henkilötietojen lisäksi ohjelman komentoja, joiden selville saaminen on yksi askel lähemmäs ohjelman hyväksikäyttöä. Salaus ei kuitenkaan välttämättä estä sitä, että ulkopuoliset käyttäisivät komentoja. Toistohyökkäys (replay-attack) tallentaa kohdelaitteelle tai ohjelmalle lähetettyjä viestejä ja lähettää ne uudelleen kohteelle (Nagamalai ym. 2005,

s. 173-174). Jos samanlainen salattu viesti aiheuttaa aina saman toiminnon, ei salaus suojaa toistohyökkäykseltä ja ulkopuolinen voi käyttää kohdetta purkamatta salausta. Yksi tapa estää toistohyökkäys on käyttää viestissä laskuria, jolloin salattu viesti on jokaisella lähetyskerralla erilainen ja toistohyökkäys on torjuttu.

VPN Kun käytetään VPN:ää, niin viritetään salattuja yhteyksiä julkisen verkon yli ja ollaan sitä kautta yhteydessä luotetun, yksityisen verkon laitteisiin ja palveluihin. Tämä yhteys voidaan tehdä verkon eri tasoilla, esimerkiksi OSI-mallin linkki-, verkko- ja sovelluskerroksille on omat tapansa tehdä yksityinen virtuaalinen verkko (Singh, Samaddar ja Misra 2012).

Autentikointi Kun on estetty ulkopuolisten sekaantuminen, pitäisi asianomaisten käyttäjien ja ohjelmien päästä käyttämään suojeltua kohdetta. Autentikoinnin avulla pyritään varmistamaan, että sisään ei lasketa ketä tahansa, vaan vain oikeutetut pääsevät kiertämään esteet. Käyttäjien autentikointi on haasteellista ja sitä on käsitelty myös lääkintälaitteiden kannalta (ks. Halperin, Heydt-Benjamin, Fu ym. 2008; Rostami, Juels ja Koushanfar 2013; Rostami ym. 2013).

Tuntemattomuuden turva (Security through obscurity) Luottaminen siihen, että hyökkääjät eivät tunne järjestelmää eivätkä sen toimintaa on turvallisuuden suunnittelun kannalta virhe (Burleson ym. 2012, s. 15). Tuntemattomuuden turvan toimimattomuus on todettu jo 1800-luvulla: Burleson ym. (2012, s. 15) Kerckhoffsin periaatteeseen (Kerckhoffs 1883). Kerckhoffsin periaatteen mukaan salausjärjestelmän tulee mm. pystyä salaamaan viestejä, vaikka salausjärjestelmän rakenne ja toiminta on tiedossa, kunhan avain on turvassa. Tätä periaatetta voidaan laajentaa koskemaan muitakin järjestelmiä, jolloin esimerkiksi lääkepumpun toimintaa ei edes laitteen tekijöiden pitäisi pystyä häiritsemään tai tietoja vakoilemaan, kunhan salasanat ovat turvassa. Tuntematon kytkentä tai protokolla hidastaa toki hyökkääjiä, mutta kun protokolla on selvitetty, katoaa turva kertaheitolla. Salasanojen ja avaimien avulla salatussa viestinnässä hyökkääjä joutuu murtamaan jokaisen avaimen erikseen.

3.3.2 Eheys

Ehyttä tieto ei ole muuttunut sen jälkeen, kun se on tallennettu tai lähetetty. Tieto on voinut muuttua tahattomasti esimerkiksi sähköisen kohinan myötä tai joku on tahallisesti muokannut sitä. Terveydenhuollon kannalta on kriittistä, että kirjatut lääkemääräykset ja annetut annostie-

dot ovat oikeita eivätkä ne ole muuttuneet matkan varrella. Vääriin tietoihin pohjautuva hoito voi vaarantaa potilaan hyvinvoinnin.

Yksi tapa varmistaa viestien eheys satunnaisien virheiden varalta on käyttää CRC:itä (cyclic redundancy checks) eli syklisiä, ylimääräisiä tarkistuksia. CRC:n ideana on nähdä viesti lukuna ja lisätä tarkistusosa siten, että jakolaskut menevät tasan vain kuin viesti on päässyt perille virheettömästi (Peterson ja Brown 1961, s. 231; Stigge ym. 2006, s. 2) . CRC-tarkistukset eivät kuitenkaan paljasta tahallista muokkaamista, sillä uusi CRC on helppo laskea väärennettyyn viestiin (Stigge ym. 2006, s. 17; Peris-Lopez ym. 2009, s. 374).

Tiedon tahallisen muuttamisen havaitsemiseen tai estämiseen on eri keinoja. Esimerkiksi vesileimoina voidaan piilottaa röntgenkuvaan tietoja, joiden perusteella voidaan päätellä, onko kuvaa peukaloitu (Coatrieux ym. 2000, s. 252). Lisäksi salaus estää tiedon huomaamattoman manipuloinnin, jos salausavainta ei olla murrettu. Jos ei tiedetä datan merkitystä, sen muuttaminen toiseksi järkeväksi versioksi on erittäin vaikeaa.

Kiistämättömyys Yksi eheyteen liitettävissä oleva ominaisuus on kiistämättömyys. Kiistämättömyys on ”kyky todistaa väitetyn tapahtuman tapahtuminen ja entiteetit, jotka saivat sen aikaan” (*ISO/IEC 27000:2016* 2016, pykälä 2.54). Kun kiistämättömyys toimii, voidaan esimerkiksi yksilöidä henkilö, joka poisti asiakastietokannan sisällön. Kiistämättömyys auttaa sisäpiiriläisuhan hillitsemisessä. Entiteetti ei välttämättä rajoitu ihmisiin, vaan voidaan myös todistaa, mikä ohjelma lähetti henkilökunnan tiedot ulkopuoliselle palvelimelle.

3.3.3 Saavutettavuus

Tiedon, laitteiden ja ominaisuuksien tulee olla niihin oikeutettujen saavutettavia, eli käytettävissä. Jos diagnostiikkatietoihin ei päästä käsiksi, terveydenhuollossa ollaan ongelmissa. Samoin, jos laite ei toimi niin kuin sen pitäisi ja toiminto, esimerkiksi veren happisaturaation mittaaminen, ei ole käytettävissä, joudutaan näkemään ylimääräistä vaivaa hoidettaessa.

Palvelimien saavutettavuutta uhkaavat palvelunestohyökkäykset, eli DoS-hyökkäykset (Denial of Service). Yksi tapa estää palvelimen normaali toiminta on lähettää sille valtavasti palvelupyyntöjä, jolloin palvelin ruuhkautuu eivätkä oikeat asiakkaat pääse käsiksi palvelimeen. Tätä voidaan estää palomuureilla, jotka jättävät välittämättä viestejä tietyn säännöstön

mukaan. Esimerkiksi jos yhdestä osoitteesta tulee valtavalla nopeudella pyyntöjä, osoitteessa olevan laitteen saatetaan olettaa yrittävän DoS-hyökkäystä. Sitten hylätään siltä tulevat viestit tietyksi ajaksi. Tässä lähestymistavassa on vaarana, että estetään oikeita asiakkaita, joiden toistuvat yhteydenottoyritykset johtuvat jostain viattomasta syystä, esimerkiksi huonosta yhteydestä.

3.4 Testaaminen

Tässä kappaleessa käydään läpi testaamista ja sen eri tyyppejä. “Ohjelmiston testaaminen on prosessi tai sarja prosesseja, joiden tarkoitus on varmistaa, että tietokonekoodi tekee, mitä sen on tarkoitus tehdä, ja kääntäen, että se ei tee mitään, mitä sen ei ole tarkoitus tehdä. Ohjelmiston tulee olla ennustettavaa ja johdonmukaista eikä sen pidä yllättää käyttäjää” (*The Art of Software Testing* 2011, s. 2).

Yksi testaamisen rajoite tiivistyy Edsger W. Dijkstran lausahdukseen: “Testaaminen tuo esiin virheiden olemassaolon, ei niiden puutetta” (Randell ja Buxton 1970, s. 21). Eli jos laite tai ohjelmisto läpäisee testin, voidaan todeta, että testattuja virheitä ei ole. Se ei tarkoita, että laite tai ohjelmisto olisi virheetön. Osoitustestien läpäisyn jälkeen voidaan todeta, että vaatimukset täytetään. Tällöin vaatimusten kattavuus ja jokaisen vaatimuksen testien kattavuus vaikuttavat testien hyödyllisyyteen ja vakuuttavuuteen.

Testien huono laatu on myös ongelmana. Esimerkiksi testien valinnassa päädytään joskus käyttämään testejä, joista ohjelmisto tai laite selviää (Gelperin ja Hetzel 1988, s. 688). Tämä ei edistä edes virheiden löytymistä, saati testaustulosten vakuuttavuutta ohjelmiston laadusta. Tätä yritetään vähentää kehittämällä menetelmiä, joita seuraamalla testit saataisiin mahdollisimman kattavaksi.

ISO/IEC 15408-3:2008 (2008, pykälä 5.2) perustaa turvallisuudesta vakuuttumisen arviointiin, mutta on avoin muillekin menetelmille, kunhan ne on todettu toimiviksi. Arviointi voidaan samaistaa testaamiseen: katsotaan, onko jokin niin kuin sen pitäisi. Testaaminen ei ole siis täydellinen ratkaisu laadun ja turvallisuuden varmistamiseen, mutta se tällä hetkellä yleisimmin hyväksytty tapa.

Testaaminen on hyvin monimuotoista ja seuraavaksi sitä jaotellaan testien lähteen, testauksen kohteen ja käytettyjen tekniikoiden mukaan. Testien lähde määrittelee, onko kyseessä mustalaatikkotestaamista, valko- eli lasilaatikkotestaamista vai harmaalaatikkotestaamista. Mustalaatikkotestaamisessa testaaja ei käytä tietoa järjestelmän sisäisestä rakenteesta hyödykseen vaan kehittää testit ulkoisista vaatimuksista (Ammann ja Offutt 2008, s. 21). Tätä voi tehdä esimerkiksi ulkopuolinen testaaja. Valkolaatikkotestaamisessa puolestaan testataan koodia: käydään läpi koodin osia ja testataan siinä havaittuja mahdollisia ongelmakohtia (Ammann ja Offutt 2008, s. 21). Tällöin testaaja lienee kehittäjä tai testaa kehittäjän toimeksiannosta kaiken avun saaden. Harmaalaatikkotestauksessa nojaudutaan koodia korkeamman tasoisempaan rakenteen tarkasteluun (Linzhang ym. 2004, s. 3). Mustalaatikkotestaus on käyttäjän näkökulmasta testaamista, kun taas lasilaatikko on kehittäjän näkökulmasta ja harmaalaatikko suunnittelijan silmin (Linzhang ym. 2004, s. 3).

Testaamista tehdään järjestelmän eri tasoilla: yksikkötesti testaa yksittäistä osaa, integraatiotesti osien yhteen toimimista ja järjestelmätestaus koko järjestelmän toimivuutta (“Guide to the Software Engineering Body of Knowledge 2004 Version” 2004, kohdat 2.1 -2.1.3). Turvallisuutta ja muita laadullisia ominaisuuksia testataan järjestelmätestauksen skaalassa (“Guide to the Software Engineering Body of Knowledge 2004 Version” 2004, kohta 2.1.3).

Kohteen lisäksi testausta voidaan luokitella tarkoituksen mukaan. Gelperin ja Hetzel (1988, s. 688) jaottelevat testausmalleja seuraavasti: *Osoitusmalli* “varmistaa, että ohjelmisto täyttää vaatimuksensa”. *Tuhoamismallissa* yritetään löytää virheet toteutuksessa, ja *arviointimallissa* yritetään havaita toteutuksen virheiden lisäksi virheet vaatimuksissa ja rakenteessa. *Ehkäisymallissa* yritetään “estää vaatimuksien, rakenteen ja toteutuksen viat”. Tavoitteet voidaan siis tiivistää varmistamiseen, virheiden löytämiseen ja estämiseen. Tosin nämä eivät ole toisiaan poissulkevia lähestymistapoja (Gelperin ja Hetzel 1988, s. 688), melkeinpä painotuseroja.

Ohjelmiston tai laitteen testaaminen standardeja vasten on luonteeltaan osoittavaa, enemmän kuin virheitä etsivää tai ennalta ehkäisevää. Virheiden löytäminen ennen markkinoille saamista on tärkeää, mutta standardien noudattaminen on se, jota tavoitellaan. Esimerkiksi eurooppalaisen CE-merkinnän saaminen edellyttää standardien noudattamista ja merkin myötä myyminen helpottuu.

Testaamiseen on monia tekniikoita, jotka voidaan jaotella sen mukaan, mihin ne perustavat testien kehittämisen (“Guide to the Software Engineering Body of Knowledge 2004 Version” 2004, kohta 3). *Testaajan intuitioon* perustuvat tekniikat eivät ohjeista tapausten kehittämiseen juurikaan vaan luottavat testaajaan. *Määrityksiin* pohjautuvat tekniikat nojaavat ohjelmalle annettuihin vaatimuksiin ja sen tunnettuihin ominaisuuksiin. Esimerkiksi päätöspuutekniikkassa (“Guide to the Software Engineering Body of Knowledge 2004 Version” 2004, kohta 3.2.3) käydään läpi ohjelman tilat ja niiden tulokset systemaattisesti. *Koodiin* perustuvat menetelmät pyrkivät käymään koodin läpi mahdollisimman kattavasti. *Virhekeskeiset* tekniikat pyrkivät huomaamaan todennäköisimpiä virheitä esimerkiksi arvaamalla (“Guide to the Software Engineering Body of Knowledge 2004 Version” 2004, kohta 3.4 ja 3.4.1). *Käyttöä* imitoivat tekniikat pyrkivät toistamaan oikeaa käyttöä mahdollisimman tarkasti haittaavien virhelähteiden löytämiseksi (“Guide to the Software Engineering Body of Knowledge 2004 Version” 2004, kohta 3.5). *Ohjelman luonteeseen* perustuvat tekniikat käyttävät hyväksi ominaisuuksia, joita ei ole kaikilla ohjelmilla (“Guide to the Software Engineering Body of Knowledge 2004 Version” 2004, kohta 3.6). Tällaisia ovat esimerkiksi olio-ohjelmointiin perustuvat testit, jotka eivät sovellu funktionaalisen ohjelman testaamiseen (“Guide to the Software Engineering Body of Knowledge 2004 Version” 2004, kohta 3.6). *Valikoivat ja yhdistelevät* tekniikat hyödyntävät useampaa tyyliä testatakseen mahdollisimman kattavasti (“Guide to the Software Engineering Body of Knowledge 2004 Version” 2004, kohta 3.7).

Testaamista voidaan yleensä tehdä tekniikasta riippumatta eri järjestelmällisyysasteilla. Ad hoc -testaaminen on yksi tyypillisimmistä tavoista testata (“Guide to the Software Engineering Body of Knowledge 2004 Version” 2004, kohta 3.1.1). Siinä ei siis tehdä järjestelmällisesti, johonkin prosessiin nojaten. Se perustuu testaajan “taitoon, intuitioon ja kokemukseen” ja sopii erityistapausten havaitsemiseen, joihin järjestelmälliset testit eivät välttämättä päätyisi (“Guide to the Software Engineering Body of Knowledge 2004 Version” 2004, kohta 3.1.1). Testaamisessa kannattaa kuitenkin pyrkiä järjestelmällisyyteen ja prosessin määrittelyyn. Silloin testaaminen on toistettavaa, hallittavaa, parannettavaa ja se voidaan opettaa nopeasti (Perry 2006, s. 153-154).

Turvallisuuden testaaminen on työlästä, joten siinä tulee keskittyä helpoimmin hyväksikäytettävien reittien turvaamiseen (Perry 2006, s. 733). Haavoittuvuuksia voivat aiheuttaa laitteesta

ja laitteeseen liikkuva data, fyysinen pääsy laitteelle, pahantahtoinen käyttö, testausprosessit, tietokoneohjelmat, käyttöjärjestelmän oikeudet ja eheys, toisena esiintyminen sekä tallennusvälineet (Perry 2006, s. 736-737).

4 Lääkintälaitteet

Lääkintälaitteiden kirjo on valtava: kaikki hoitoon ja diagnosointiin tarkoitetut tarvikkeet laastareista tekolonkkaan ja sydämentahdistimista ihosyöpäkasvaimia tunnistaviin ohjelmiin kuuluvat tämän nimikkeen alle. Tässä työssä kuitenkin keskitytään elektronisiin lääkintälaitteisiin, joihin liittyy fyysinen laite, joten pelkät ohjelmistot rajataan ulkopuolelle. Seuraavassa on lääkintälaitteiden määritelmä Suomen lain kannalta.

(*Laki terveydenhuollon laitteista ja tarvikkeista 629/2010* 2017)

> Tässä laissa tarkoitetaan:
>
> 1) terveydenhuollon laitteella instrumenttia, laitteistoa, välinettä, ohjelmistoa, materiaalia tai muuta yksinään tai yhdistelmänä käytettävää laitetta tai tarviketta, jonka valmistaja on tarkoittanut käytettäväksi ihmisen:
>
> a) sairauden diagnosointiin, ehkäisyyn, tarkkailuun, hoitoon tai lievitykseen;
>
> b) vamman tai vajavuuden diagnosointiin, tarkkailuun, hoitoon, lievitykseen tai kompensointiin;
>
> c) anatomian tai fysiologisen toiminnon tutkimiseen, korvaamiseen tai muunteluun; taikka
>
> d) hedelmöittymisen säätelyyn;

Diagnosointia voidaan nopeuttaa elektronisilla mittareilla. Esimerkiksi anemia voidaan todeta tai poissulkea nopeasti vastaanotolla olevan hemoglobiinimittarin avulla laboratorioon kuljettamisen sijaan. Sydänsähkökäyrä, EKG, voidaan mitata pienemmällä laitteella, kun tulokset tallennetaan digitaaliseen muotoon paperille piirtämisen sijaan. Magneettikuvaus on diagnosointiväline, jota ei olisi olemassa ilman tietotekniikkaa. Magneettikuvauksessa potilas makaa putkessa, jolla luodaan muuttuva magneettikenttä. Tätä magneettikenttää havainnoidaan ja sen muutoksista voidaan muodostaa kuva kehon sisäisestä rakenteesta ja hyödyntää esimerkiksi aivojen tutkimisessa tai lihaksiston ja nivelten kunnon arvioinnissa.

Varsinaista hoitoakin tietotekniikka on muuttanut. Sekä akuutti että krooninen hoito ovat saaneet osansa muutoksesta. Yksi esimerkki akuutista, lyhytaikaisesta hoidosta on kammiovärinän hoidossa. Nykyaikaiset defibrillaattorit, eli sydäniskurit varmistavat, että potilaalla on kammiovärinää, ennen kuin antavat sähköiskun. Tämän ansiosta ostoskeskuksiin on voitu sijoittaa näitä laitteita maallikoiden käyttöön ("Defibrillaattorit yleistyvät kotona ja työpaikoilla" 2012). Käyttäjän ei itse tarvitse tunnistaa kammiovärinää, kun laite tekee lopullisen päätöksen sähköiskun antamisesta.

Kroonista, eli pitkäaikaista hoitoa ovat helpottaneet mukana kulkevat insuliinipumput, joiden myötä ei tarvitse enää tarvitse käsin mitata verensokeria ja annostella insuliinia. Lisäksi pumppujen käyttö on kätevyyden lisäksi tehokkaampaa kuin pistämällä annettu hoito (Bergenstal ym. 2010). Tietotekniikka mahdollistaa myös uuden hoidon krooniseen sairauteen: dialyysilaite, joka korvaa vahingoittuneen munuaisen toiminnan.

Terveydenhuoltoa voidaan turvata tietotekniikan avulla. Esimerkiksi lääkkeiden yhteisvaikutukset voivat aiheuttaa vakavaa haittaa ja tietojärjestelmät, jotka ylläpitävät tietoa näistä vaikutuksista, auttavat ammattilaisia sopivien lääkkeiden valinnassa (Neuvonen 2013). Lisäksi potilaiden tilan seuranta laitteilla voi olla jatkuvaa ja tilan huononeminen voidaan pysäyttää ajoissa, sillä laite huomaa huononemisen nopeasti. Lääkintälaiteet ovat kuitenkin haavoittuvaisia siinä missä muutkin tietotekniset laitteet. Esimerkiksi kipulääkkeen suonensisäiseen tiputusannosteluun tarkoitettu pumppu sisälsi haavoittuvuuden, joka mahdollisti koodin ajamisen laitteessa ja siten melkein vapaat kädet hyökkääjille (*CVE-2015-3955* 2015).

Mikä lääkintälaitteissa kiinnostaa pahantekijöitä? Arney ym. (2011, s. 2377) jaottelevat hyökkääjän kohteet neljään luokkaan: potilaan terveys, potilaan yksityisyys, lääkintälaitteen toimintakyky ja laitoksen kyberturvallisuus. Potilaan terveyttä tai yksityisyyttä vastaan hyökkätessä kohteena ovat ainoastaan yksittäiset potilaat, lääkintälaite ja laitoksen kyberturvallisuus puolestaan koskettavat monia (Arney ym. 2011, s. 2377).

Tarkastellaan näihin kohteisiin hyökkäämistä CIA:n silmin. Miten näiden osa-alueiden heikentäminen haittaa potilasta? Potilaan terveyttä voidaan uhata lääkintälaitejärjestelmän kautta eheyden ja saatavuuden rikkomisella. Jos lääkeannostiedot on väärennetty tietokantaan tai lääkintälaitteeseen, niiden pohjalta annettava seuraava lääke voi olla haitallinen. Toisekseen,

jos terveystietoja ei ole saatavilla ratkaisevalla hetkellä, potilaan henki voi olla vaarassa. Myös laitteen toimintojen estäminen voi olla haitaksi potilaan terveydelle. Luottamuksellisuuden puute ei vielä yksinään aiheuta terveydelle vaaraa, mutta tietoja voidaan kuitenkin käyttää potilasta vastaan myöhemmin.

Potilaan yksityisyyden loukkaaminen seuraa järjestelmän luottamuksellisuuden puutteellisuudesta. Arney ym. (2011, s. 2377) antaa esimerkkihyökkäyksiksi laitteen muistin tyhjentämättä jäämisen myötä tietojen lukemisen laitteesta, tietojen varastamisen vakuutushuijauksen tekemiseksi ja henkilökunnan jäsenen uteliaisuuden tyydyttämisen terveystietojen selailulla. Terveystietoja pyritään keräämään, sillä ne ovat haluttua kauppatavaraa (Humer ja Finkle 2014). Erityisen ongelmallista terveystietojen vuotaminen on siksi, että niitä ei voi muuttaa (Yao 2017). Jos saa tietoonsa, että luottokortin tunnukset on varastettu ja joku käyttää niitä, voi kuolettaa kortin ja hankkia uuden. Jos omat terveystiedot on varastettu, ei diagnoosejaan tai insuliiniannosten kokoaan voi muuttaa yhtä helposti. Terveystietojen kysyntä ei kuitenkaan ole noussut tarjonnan myötä, joten tietojen hinnat ovat pudonneet (Bing 2016).

4.1 Esineiden Internet -laitteita lääkintälaitteina

Esineiden Internet (Internet of Things, IoT) antaa paljon mahdollisuuksia lääkintälaitteille (Hu, Xie ja Shen 2013). Esineiden Internetille on monia määritelmiä. Esimerkiksi ITU:n eli kansainvälisen televiestintäliiton määritelmän mukaan Esineiden Internet on ‘’maailmanlaajuinen tietoyhteiskunnan infrastruktuuri, joka mahdollistaa kehittyneitä palveluita yhdistämällä (fyysisiä ja virtuaalisia) laitteita perustuen olemassaoleviin ja kehittyviin yhteentoimiviin tieto- ja viestintäteknologioihin” (*Recommendation ITU-T Y.2060* 2012, pykälä 3.2.2).

Tämä määritelmä on varsin laaja eikä erota esimerkiksi tavallisia tietokoneita esineiden Internetin ulkopuolelle. Ma (2011, s. 920) puolestaan määrittelee esineiden Internetin seuraavasti: “Pohjautuen perinteisiin tiedonkuljetustapoihin, mukaan lukien Internet, esineiden Internet on verkosto, joka yhdistää tavallisia fyysisiä objekteja tunnistettavilla osoitteilla siten, että se tarjoaa älykkäitä palveluita.” Tässä määritelmässä esineiden Internet -laitteiden yhteys fyysiseen maailmaan on nostettuna keskiöön.

Verkkoon kytkettyjen lääkintälaitteiden ongelmat ovat pitkälti yhteisiä esineiden Internet

-laitteiden kanssa ja ratkaisutkin voivat olla samoja. Molemmat ovat yhteydessä jonkinlaiseen tietoverkkoon ja yhdistävät fyysisen maailman kybermaailmaan. Lisäksi monet lääkintälaitteet ovat patterien ja akkujen varassa (Arney ym. 2011, s. 2378), mikä pätee myös esineiden Internet -laitteisiin (Mattern ja Floerkemeier 2010; Kaur ja Kaur 2016)

4.1.1 Virransaanti

Virran varastoiminen pattereihin ja akkuihin kasvattaa laitteen kokoa, ja sähkön tuottaminen ympäristöstä, esimerkiksi valosta ja tuulesta, ei aina ole riittävän tehokasta laitteiden tarpeisiin (Mattern ja Floerkemeier 2010). Bormann, Ersue ja Keranen (2014) jakavat sähkönsaanniltaan rajoittuneet laitteet tapahtuma-, jakso- ja elinikärajoitteisiin sekä rajoittamattomiin. *Tapahtumarajoitteiset* saavat ja käyttävät virtaa vain tietyissä tilanteissa. He antavat esimerkkinä energiaa keräävän valokatkaisijan. *Jaksorajoitteiset* saavat virtaa tietyn jakson ajan joko patterin vaihtamisen tai akun lataamisen jälkeen. *Elinikärajoitteiset* eivät saa mistään lisää virtaa, vaan ovat patterin varassa, jonka loppumisen jälkeen laitetta ei voi enää käyttää. *Rajoittamattomat* ovat kytkettynä verkkovirtaan eikä sähkönsaanti ole niille ongelmallista.

Luonnollinen seuraus sähkönsaannin vaikeudesta on se, että kulutusta minimoidaan. Turvallisuus yleensä kuluttaa sähköä, joten se on karsintavaarassa. Esimerkiksi monimutkaiset salaukset vaativat paljon laskentaa ja energiaa ja niitä pyritään välttämään.

4.1.2 Keskinäinen kommunikointi

Lääkintälaitteista suurin osa toimii yksin tai vaihtaa tietoja lähinnä saman laitevalmistajan lääkintälaitteiden kanssa (Arney ym. 2011, s. 2376; Venkatasubramanian ym. 2012, s. 61).

Terveystietoja keräävät järjestelmät voidaan jakaa eri tasoihin. Kocabas, Soyata ja Aktas (2016, s. 402) jakavat järjestelmän kerätyn datan käytön perusteella neljään kerrokseen: keräämiseen, esikäsittelyyn, pilveen ja toimintaan. Keräämisen hoitavat pienet laitteet, esimerkiksi sykemittarit ja lämpötilamittarit, ja niiden keräämä data lähetetään eteenpäin esikäsittelyyn. Tämän jaon pääasiallisiin sensoreihin ja tiedon esikäsittelijöihin, nostivat esille myös Pantelopoulos ja Bourbakis (2010).

Nämä eritasoiset laitteet ovat yhteydessä tietoverkkoon ja toisiinsa. Eri osasilla on erilaiset haasteet. Pilvi on todennäköisesti osa laajempaa verkkoa ja siten herkemmin hyökkäyksen kohteena. Toisaalta pienillä sensoreilla on niukasti resursseja: joko muistia tai laskentatehoa on vähän tai virrankulutus on pidettävä mahdollisimman pienenä. Pilvipalvelin voi käyttää edistyneempiä salausmenetelmiä ja muita keinoja turvaamaan itseään, mutta yksittäisen sensorin keinot ovat vähäisemmät. Lisäksi pieni sensori saatetaan varastaa, jolloin sen toimintatapa voidaan selvittää ja mahdollisesti istuttaa siihen oma ohjelma.

4.2 Lääkintälaitteiden erityishaasteet

Tiedon luottamuksellisuudella, eheydellä ja saatavuudella on pieniä merkityseroja terveydenhuollossa (Krens, Spruit ja Urbanus 2013). Terveystiedon eheys ja saatavuus mahdollistavat sen, että hoito on oikeaa ja se annetaan ajallaan. Tiedon eheys ja saatavuus siis nousevat elämän ja kuoleman kysymyksiksi. Näin luottamuksellisuus, joka nousee muussa tietoturvakeskustelussa erityisesti esille (Krens, Spruit ja Urbanus 2013, s.325), ei välttämättä ole keskiössä. Luottamuksellisuus on kuitenkin tärkeää potilaan muun elämän kannalta, sillä vuotaneiden terveystietojen julkitulo voi aiheuttaa esimerkiksi syrjintää. Terveystiedot ovat kauppatavaraa (Humer ja Finkle 2014), joskin niiden hinnat ovat laskeneet tarjonnan myötä (Bing 2016).

4.2.1 Implantit

Lääkintälaitteiden erityistyyppinä ovat implantit. Implantti on laite, joka liitetään kehoon. Esimerkiksi sydämentahdistimet, jotkin insuliinipumput ja sisäkorvaistutteet ovat tällaisia laitteita. Monesti implanttien tarkoitus on toimia jatkuvasti ja pitkän aikaa. Joko hoidon on oltava jatkuvaa, kuten sisäkorvaistutteen tapauksessa, tai sitä on annettava säännöllisin väliajoin, kuten insuliinipumppu tekee. Myös potilaan tilaa voidaan valvoa jatkuvasti ja mahdollisesti antaa tarvittaessa apua. Rytmihäiriötahdistimet ovat tällaisia laitteita, jotka valvovat potilaan tilaa, sykettä, ja havaitessaan vaarallisen tilan, rytmihäiriön, ne toimivat ja antavat tilanteen tasoittavan sähköiskun (Rostami, Juels ja Koushanfar 2013; Halperin, Heydt-Benjamin, Ransford ym. 2008). Implanttien haastavuuteen kyberturvallisuuden näkökulmasta vaikuttaa mm. seuraavat tekijät: rajoitukset kokoon ja virrankulutukseen sekä langattomuus.

Joihinkin implantteihin, esimerkiksi rytmihäiriötahdistimiin, ollaan langattomasti yhteydessä ohjelmoijalla (Halperin, Heydt-Benjamin, Fu ym. 2008, s. 129). Langattomalla ohjelmoijalla voidaan ilman leikkausta muuttaa implantin toimintaa ja ladata sen keräämää dataa muuhun käyttöön (Halperin, Heydt-Benjamin, Fu ym. 2008). Langaton viestintä on turvattomampaa kuin langallinen (Radack ja Kuhn 2012), mutta kehon sisällä oleviin laitteisiin se on kätevä vaihtoehto. Langaton viestintä on kuitenkin altis kuuntelulle ja viestien toistamiselle, eli replay-hyökkäykselle. Tällä tavalla rytmihäiriötahdistin saatiin antamaan tarpeettomasti sähköiskuja (Halperin, Heydt-Benjamin, Ransford ym. 2008). Lisäksi muut langattomat verkot voivat aiheuttaa häiriöitä. Tri, Trusty ja Hayes (2004) tutkivat, voidaanko WLAN- verkolla häiritä sydämentahdistimia ja onnellinen lopputulos oli, että yhtään laitetta ei saatu häirittyä.

Kehoon istutettavien laitteiden tulee olla mahdollisimman pieniä, jotta ne haittaisivat potilasta mahdollisimman vähän. Mahdollisimman pienien komponenttien ja akkujen käyttö rajoittaa implanttien laskentatehoa ja hyväksyttävää virrankulutusta. Joidenkin implanttien patterien vaihtaminen tai akkujen lataaminen vaatii leikkausta, esimerkiksi sydämentahdistimet ovat tällaisia (Rostami, Juels ja Koushanfar 2013; Halperin, Heydt-Benjamin, Fu ym. 2008). Turvatoimet vaativat yleensä laskentatehoa ja virtaa, joten turvallisuus on jälleen ristiriidassa muiden ominaisuuksien kanssa. Lisävirta implanteille vaatisi käytännössä akun suurentamista. Implantin vaatimaa koloa tuskin suurennetaan ilman hyviä perusteluita.

4.2.2 Turvallisuusvaatimukset

Lääkintälaitteiden turvallisuudelle on vaatimuksia myös lain puolesta. EU-tasolla *Lääkintälaitedirektiivi* (1993, Liite I, kohta 1) edellyttää turvallisuutta seuraavanlaisesti:

> Laitteet on suunniteltava ja valmistettava siten, että ne eivät suunnitelluissa olosuhteissa ja tarkoituksessa käytettyinä vaaranna potilaiden terveydentilaa ja turvallisuutta eikä käyttäjien tai tarvittaessa muiden henkilöiden turvallisuutta ja terveyttä, jos niiden käyttöön mahdollisesti liittyvät riskit ovat potilaalle aiheutuvaan etuun nähden hyväksyttäviä ja yhteensopivia terveyden ja turvallisuuden suojelun korkean tason kanssa.

4.2.3 Liian tiukka turvallisuus?

Voiko lääkintälaite olla liian kyberturvallinen? Lääkintälaitteiden ja erityisesti elintärkeiden implanttien kanssa kyberturvallisuuden ja järjestelmän tarvittavan avoimuuden taspainoilu on erityisen haastavaa. Molemmissa ääripäissä ihmishenkiä on vaakalaudalla. Hätätilanteessa implanttien nopea ja helppo uudelleenohjelmoiminen voi pelastaa hengen, mutta liian avoin laite altistaa pahantahtoisille hyökkäyksille (Rostami ym. 2013, s. 2; Rostami, Juels ja Koushanfar 2013, s. 1; Halperin, Heydt-Benjamin, Fu ym. 2008, s. 30).

Jos blogin palvelimen asetuksia ei voida muokata, harvoin ihmishenkiä on vaarassa. Tiukka kontrolli, joka mieluummin sulkee hyväntahtoisen tekijän ulos kuin päästää pahantahtoisen sisään, voisi blogin tapauksessa olla parempi. Avoin järjestelmä, johon pääseminen ei vaadi salasanaa tai muuta autentikointia on helposti käytettävissä ja muokattavissa, mutta samalla helpottaa hyökkääjien sisäänpääsyä. Tasapainoilu asiallisten käyttäjien käytön helppouden ja väärinkäytön vaikeuden välillä on haastava ongelma.

IEC/TR 80001-2-2:2012 (2012) viittaa *Break-Glass* (2004)-raporttiin, joka käy läpi syitä, miksi laitteissa tulisi olla tapa päästä käyttämään ilman autentikoitumista, ja antaa mallin sellaisen järjestelmälle. Raportti ehdottaa esitehtyjä, salaisia käyttäjätunnuksia. Niiden käyttäjätunnus on helppo ja salasana on vaikea murtaa, mutta helppo käyttää hätätilanteessa. Käyttäjätunnus ja salasana tulisi säilyttää siten, että niiden ottamisesta jää jälki, esimerkiksi rikottavan lasin takana tai lukkojen takana. Käyttäjätunnukset tulisi myös poistaa toiminnasta mahdollisimman pian käytön jälkeen, kun ne eivät enää ole salaisia. Inhimillisyys ja mahdolliset käytettävyyden ongelmat nousevat esiin raportissa. Siinä kerrotaan, että jos hätätunnuksia käytetään usein, ongelma lienee autentikointijärjestelmässä. Kun tietojärjestelmän kyberturvallinen käyttö estää hoitamisen, kyberturvallisuus heitetään ikkunasta.

4.3 Turvallisuuden parantamisehdotuksia

Kirjallisuudessa ehdotukset lääkintälaitteiden kyberturvallisuuden parantamiseksi voi katsoa jakautuvan kahteen tyyppiin: joko ehdotetaan konkreettisia, yksittäisiä keinoja turvata laitteita tai keskitytään laitteiden kehitysprosessiin parantamiseen. Yksittäisiä keinoja ovat esimerkiksi salausalgoritmit ja autentikoinnin kehittäminen (esim. Rostami, Juels ja Koushanfar

2013). Kehitysprosessin parantamisessa keskitytään siihen, että laitteesta saadaan alun alkaen turvallinen.

Rostami ym. (2013) käyvät katsauksessaan läpi ehdotettuja tapoja implanttien kommunikoinnin turvaamiseksi. He jakavat nämä menetelmät avaintenhallintaan ja luotettavan laitteen hyödyntämiseen. Rostami ym. (2013, s. 2) arvioivat, että avainten jakaminen laitteille etukäteen ja avainten hallinnointi olisi epäkäytännöllistä. Ratkaisut avainten turvalliseen jakamiseen implantin ja ohjelmoijan välillä nojaavat siihen, että ohjelmoija on kosketuksissa implantin käyttäjään.

Rostami ym. (2013) jakoivat avaimiin perustuvat menetelmät kahteen luokkaan. Ensimmäisessä tavassa implantti luo avaimen ja lähettää sen ohjelmoijalle käyttäjän kehon kautta, esimerkiksi äänenä (Halperin, Heydt-Benjamin, Ransford ym. 2008) tai sähköisenä viestinä (Zimmerman 1996). Toinen tapa on luoda avaimet kehon signaalien avulla. Esimerkiksi Rostami, Juels ja Koushanfar (2013) esittävät, että implantti ja ohjelmoija seuraavat sykettä ja muodostavat tiettyjen sääntöjen pohjalta avaimet. Jos nämä avaimet ovat riittävän samanlaiset, oletetaan, että ohjelmoija on kosketusyhteydessä käyttäjään ja siten sallittu käyttäjä. Tämän hyväksynnän jälkeen avaimia käytetään salaamaan langaton yhteys. Lisäksi implanttien langattoman viestinnän suojaamiseksi on ehdotettu radioliikenteen häirintälaitteita, jotka estäisivät ulkopuolisten kommunikoinnin implantin kanssa (ks. Denning, Fu ja Kohno 2008; Gollakota ym. 2011).

Kehitysvaiheessa voidaan edistää tuotteen turvallisuutta puurakenteisella vakuutusperuste (assurance case) -päättelyllä. Siinä otetaan juurioletus, esimerkiksi “Laite on turvallinen” ja pilkotaan se pienempiin osiin, jotka vuorostaan pilkotaan pienemmiksi, kunnes päästään toteutettaviin ja testattaviin kohtiin (A. Finnegan ja F. McCaffery 2014, s. 222). Tätä päättelyä käytetään monilla muillakin ”turvallisuuskriittisillä toimialoilla, kuten autojen, rautateiden puolustuksen ja ilmailun” turvaamiseen (A. Finnegan ja F. McCaffery 2014, s. 220).

Ainakin otsikoista ja tiivistelmistä päätellen standardeissa keskitytään nostamaan kyberturvallisuus keskiöön jo kehitysvaiheessa, juurikin vakuutuspäättelyyn nojaten. Joten turvallisuuden takaamisessa keskitytään laitteen kehittämiseen ja turvallisen suunnittelun edistämiseen.

5 Kyberturvallisuuden standardit

Standardien tavoitteina on parantaa tuotteita, laskea kustannuksia ja edistää kommunikaatiota (Kajava ym. 2006, s. 2091). Esimerkiksi ulkoistamisen onnistumisessa standardit ovat avainasemassa tukemassa yhteisymmärrystä (Kajava ym. 2006, s. 2092). Lisäksi standardienmukaisuus auttaa saamaan asiakkaiden luottamuksen (Beckers ym. 2014).

Kajava ym. (2006, s. 2094) tarkastelevat tietotekniikan turvallisuusstandardeissa havaittavaa jakoa teknisiin ja hallinnollisiin standardeihin. Heidän mukaansa tekniset standardit mahdollistavat laitteiden toimimisen yhdessä ja hallinnolliset standardit pyrkivät parantamaan yritysten toimivuutta. Esimerkiksi ISO 27000 -standardiperhe käsittelee tietoturvallisuuden hallintajärjestelmiä ja on siten hallinnollinen. Selkeästi tekninen standardi on puolestaan IEEE 802.11n-2009, joka määrittelee langattoman lähiverkon toiminnan.

Standardeissa on havaittu olevan yleisiä ongelmia. Standardien yleismaailmallisuus, vaihtuviin tilanteisiin mukautumattomuus ja mitattavien vaatimuksien puute heikentävät standardien hyödyllisyyttä (Siponen ja Willison 2009, s. 287). Liian yleistasoiset standardit eivät välttämättä tue tekemistä vaan ovat kaukaisia tavoitteita. Standardien käyttämistä hillitsee standardien suuri määrä, ristiriitaisuus keskenään ja muu sirpaloituminen (Cheremushkin ja Lyubimov 2010, s. 12). Cheremushkin ja Lyubimov (2010, s. 12) pohtivat, että ristiriitaisuudet voisivat johtua tavasta, jolla kansainväliset standardit tehdään: pohjalta lähtien eikä yleiskuvasta johtaen.

Standardien valitsemisessa hankkimista varten oli hieman vaikeuksia, sillä tätä tutkielmaa tehdessä oli välillä haastavaa päätellä standardin olennaisuutta omaan työhön pelkästään niiden nimien ja lyhennelmien perusteella. ISO tarjoa standardeista esikatseltavaksi osan, jota rajattaessa täytyy varmasti taiteilla ostajan helpottamisen ja tiedon tarpeettoman paljastamisen välillä. Esimerkiksi ISO/IEC 15408-1 sisältää kohdeyleisön kertovan osan, mutta se ei sisälly esikatseluun (*ISO/IEC 15408-1:2009* 2009, s. 20). Sen sisällyttäminen voisi helpottaa standardien tarpeellisuuden päättelyä. Tässä pro gradu -tutkielmassa on lyhennelmiä aiheeseen liittyvistä standardeista, jotka toivottavasti auttavat muita löytämään tarvitsemansa tai jättämään aiheestaan ohi menevät hankkimatta. Myös Beckers ym. (2014) huomasivat

ongelman standardien oleellisuuden hahmottamisessa ja kehittivät mallin, joka avaa standardien keskinäisiä suhteita ja niiden sisältöjä. Standardien sisältöjen hahmottaminen on siis tiedostettu ongelma.

5.1 ISO/IEC 15408

ISO/IEC 15408-1:2009 (2009) on tietoteknisten tuotteiden tietoturvallisuuden arviointistandardi. Sen tavoitteena on luoda yhtenäinen kieli, jotta eri turvallisuusarviointien tuloksia voitaisiin vertailla (*ISO/IEC 15408-1:2009* 2009, s. iv). Standardista on hyötyä kuluttajille mm. valmiiden vaatimusten muodossa: ei tarvitse kehittää omia vaatimuksia kun oleellisimpia turvallisuusaspekteja on kirjattuna valmiiksi (*ISO/IEC 15408-1:2009* 2009, pykälä 5.3.1). Kehittäjille on tarkemmat vaatimukset, ja turvallisuuden arvioijille standardi antaa kriteerit.

5.1.1 Määritelmät ja yleinen käyttö

ISO/IEC 15408-1:2009 (2009) käy tarkasti läpi arvioitavan kohteen (Target of Evaluation, TOE) määrittelyn. Arvioitava kohde voi olla monenlainen: se voi sisältää sekä ohjelmistoa, että fyysisiä asioita tai vain toista. Standardissa esimerkeiksi annetaan pelkkä ohjelmisto, pelkkä laite ja paketti, joka sisältää laitteen, sen ohjelmistot ja käyttöohjeet (*ISO/IEC 15408-1:2009* 2009, s. 23, pykälä 5.2). Kohdetta voidaan rajata edelleen: Jos testataan laitetta, jossa on asetuksia, tulee ennen testausta määritellä, mitkä asetusvaihtoehdot kuuluvat TOE:hen, arvioinnin kohteeseen. Otetaan esimerkiksi tietokone, jonka turvallisuutta tutkitaan. Oletetaan, että tietokoneesta löytyy asetuksista vaihtoehto, että kysytäänkö kirjauduttaessa salasanaa. Tämä erittäin turvaton vaihtoehto voidaan rajata arvioinnin ulkopuolelle, kunhan se kirjataan ylös ja sitä ei käytetä.

ISO/IEC 15408-1:2009 (2009) keskittyy CIA:han, eli luottamuksellisuuteen, eheyteen ja saavutettavuuteen. Standardin sanoin: ”ISO/IEC 15408 käsittelee resurssien suojelua luvatonta paljastamista, muokkausta ja käytön menetystä vastaan” (*ISO/IEC 15408-1:2009* 2009, s. vi). Suojeltavaa kohdetta kutsutaan resurssiksi (asset). Resurssilla tarkoitetaan jotain arvossa pidettyä asiaa (*ISO/IEC 15408-1:2009* 2009, s. 23, pykälä 6.2). Resurssi voi olla konkreettinen, kuten jokin laite, sen sisältämät tiedot tai oven lukon toimivuus. Resurssien abstraktimmaksi

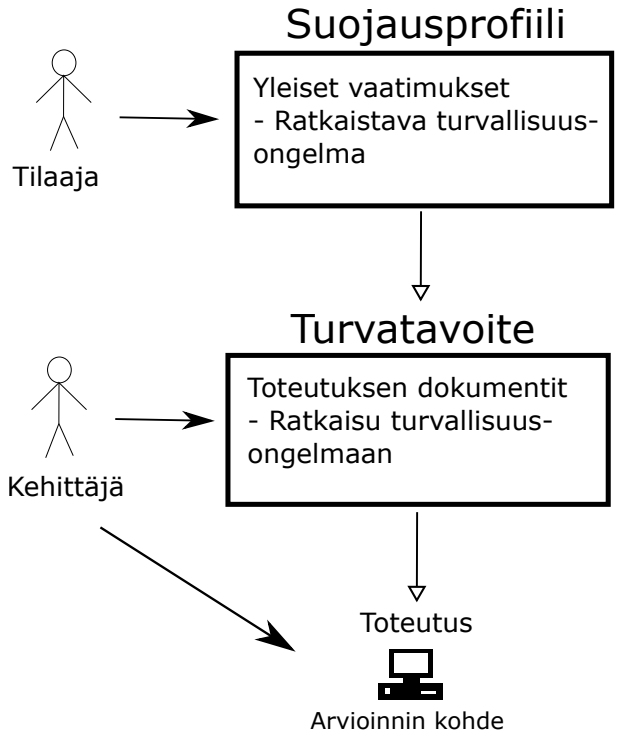
esimerkiksi nostettiin vaalien äänten aitous (*ISO/IEC 15408-1:2009* 2009, s. 23, pykälä 6.2).

ISO/IEC 15408 pyrkii palvelemaan sekä kuluttajia että kehittäjiä. Näiden ryhmien tarpeet teknisille yksityiskohdille ovat erilaiset, ja samojen dokumenttien kirjoittaminen sekä yleistajuisiksi että teknisesti tarkoiksi on haastava tehtävä. Tämä standardi on erottanut nämä kahden kohderyhmän kaipaamat tiedot eritasoisiksi dokumenteiksi. Erityisesti suojausprofiilit (Protection Profile, PP) tehdään kuluttajien, hankinnan ja hallinnon näkökulmasta (*ISO/IEC 15408-1:2009* 2009, pykälä 8.3). *ISO/IEC 15408-1:2009* (2009, pykälä 8.3) esittelee suojausprofiilin ylimmän tason dokumentina, joka määrittelee vaatimukset tuoteluokalle, esimerkiksi reitittimille tai verkkoliikenteen kuunteluohjelmille.

Sama pykälä esittelee turvatavoitteen (Security Target, ST), joka on seuraava askel kohti kehittäjien vaatimaa tarkuutta. Turvatavoite puolestaan koskee jo tiettyä tuotetta, esimerkiksi ASUS AC1200 -reititin tai Wireshark 2.2.7 -ohjelma. Suojausprofiili ja turvatavoite ovat hyvin samanmuotoiset dokumentit, joita erottaa niiden tarkastelutaso. Profiilissa on erilaisia vaihtoehtoisia kohtia, jotka sidotaan turvatavoitteessa tiettyihin arvoihin. Eli profiilissa kerrotaan, miten tämä vaatimus voidaan täyttää ja turvatavoitteessa määritellään, mitä kyseisessä laitteessa ollaan tehty annetuista vaihtoehdoista. Suojaprofiilien ja turvatavoitteiden suhde näkyy kuviossa 1.

Julkisia, tarkistettuja profiileja ja turvatavoitteita löytyy mm. Common Criterian omilta sivuilta (*Common Criteria* 2017). Yhdysvaltojen tietoteknisten kuluttajalaitteiden yhteensopivuutta ISO/IEC 15408:n, eli Common Criteria:n kanssa valvoo The National Information Assurance Partnership (NIAP) ja NIAP myös julkaisee turvallisuusprofiileja (*NIAP* 2017). Common Criteria -sivustolta löytyi yksi yleisesti terveystietojärjestelmille tarkoitettu suojausprofiili (*Protection Profile for Security Module of General-Purpose Health Informatics Software* 2016). Lisäksi listattuna on tarkempia, terveydenhuoltoon käytettyjen älykorttien ja niihin liittyvien järjestelmien profiileja.

ISO/IEC 15408-1:2009 (2009, pykälä 8.4) avaa suojausprofiilien ja turvatavoite-dokumenttien käyttöä. Suojausprofiileja ja turvatavoitteita on tarkoitus käyttää niin, että tuotteen tilaaja tekee tai valitsee suojausprofiilin . Kehittäjäosapuoli tekee profiilin toteuttavan turvatavoite-dokumentin . Turvatavoitteen toteuttava tuote valitaan tai kehitetään. Lopuksi varmistetaan,



Kuvio 1. Suojausprofiilien, turvatavoitteiden ja arvioinnin kohteen suhteet sekä tekijät

että se toteuttaa turvatavoitteen vaatimukset, mistä seuraa, että tuote toteuttaa suojausprofiilin vaatimukset ja tilaaja saa mitä haluaa.

5.1.2 Turvallisuuden toiminnalliset vaatimukset (SFR) ja turvallisuuden vakuutusvaatimukset (SAR)

Suojausprofiilien ja turvatavoitteiden ydinsisältöä ovat turvallisuuden toiminnalliset vaatimukset (Security Functional Requirements, SFR) ja turvallisuuden vakuutusvaatimukset (Security Assurance Requirements, SAR). *ISO/IEC 15408-2:2008* (2008) listaa joitain oleellisia turvallisuuden toiminnallisia vaatimuksia (SFR), ja *ISO/IEC 15408-3:2008* (2008) käsittelee vakuutusvaatimuksia ja muutenkin kohteen (TOE) turvallisuuden vakuuttamistapoja. Toiminnalliset vaatimukset kertovat, mitä tuotteen tulisi tehdä. Esimerkiksi käyttäjätilien väärinkäytön hankaloittamiseksi tietokoneen käyttöjärjestelmää voidaan vaatia lukitsemaan toimettoman käyttäjän tili 10 minuutin käyttämättömyyden jälkeen. Vakuutusvaatimukset listaavat testit, jotka arvioijan on tehtävä tutkiessaan, toteuttaako tuote toiminnalliset vaati-

mukset. Esimerkiksi voidaan ohjeistaa kirjautumaan tietokoneelle, olemaan tekemättä mitään 10 minuuttia ja tarkistamaan sen jälkeen, vaatiiko tietokone uudelleenkirjautumista.

Toiminnalliset vaatimukset on jaoteltu luokkiin, perheisiin ja lopuksi yksitttäisiin komponentteihin. Näille on nimeämiskäytäntö, jossa luokalla ja perheellä on kolmikirjaiminen tunnus. Ensin tulee luokka, alaviivan jälkeen perheen tunnus ja sen jälkeen komponentin numero: CLA_FAM.2. Viimeiseksi lisätään tarkistusvaatimukset: tarkemmat, testattavat vaatimukset, jolloin niihin viitattaisiin seuraavasti: CLA_FAM.2.1. Otetaan esimerkiksi toiminnalisuus, jossa käyttäjän tili lukitaan toimettomuuden myötä. Se kuuluu käyttäjän kirjautumisen hallinnasta vastaavaan luokkaan (FTA), sen alaiseen istunnon lukitsemisen ja lopettamisen perheeseen (FTA_SSL) ja on sen ensimmäinen komponentti (FTA_SSL.1) (*ISO/IEC 15408-2:2008* 2008, pykälä 16.3). Tarkastusvaatimuksia tälle ominaisuudelle on vain yksi (FTA_SSL.1.1) ja se vaatii, että näyttö tyhjennetään niin, ettei näytön sisältöä voida lukea ja että käyttäjän nimissä ei voida tehdä mitään muuta kuin kirjautua uudelleen (*ISO/IEC 15408-2:2008* 2008, pykälä 16.3.10.1).

ISO/IEC 15408-3:2008 (2008) keskittyy varsinaiseen turvallisuuden arviointiin. Se sisältää vakuutusvaatimuksia (SAR) jaoteltuna luokkiin, perheisiin ja pohjimmaisena komponentteihin, kuten toiminnalliset vaatimuksetkin (SFR). Nämä kertovat, mitä arvioijan tulee tehdä tai tarkistaa. Tässä standardissa annetaan työkaluja myös testattavien vaatimusten valintaan.

Arvioinnin vakuutustaso (Evaluation Assurance Level, EAL) on yhdestä seitsemään. Yksi on kaikkein kevyin ja halvin. Se on tarkoitettu pienen riskin kohteille, joiden turvallisuus ei ole kriittistä (*ISO/IEC 15408-3:2008* 2008, pykälä 7.3.1). Siinä ei myöskään vaadita kehittäjän yhteistyötä (*ISO/IEC 15408-3:2008* 2008, pykälä 7.3.1). Toinen taso vaatii vähän tietoja kehittäjältä, mutta ei suuria ponnistuksia (*ISO/IEC 15408-3:2008* 2008, pykälä 7.4.1). Neljäs on korkein taso, joka on järkevä olemassa olevien tuotteiden analysointiin ja parantamiseen (*ISO/IEC 15408-3:2008* 2008, pykälä 7.6.1). Korkein, seitsemäs, taso on tarkoitettu käytettäväksi kriittisten kohteiden kehittämiseen (*ISO/IEC 15408-3:2008* 2008, pykälä 7.9.1).

Eri osista koostettujen kohteiden arvioinnissa on käytettävissä koostettu vakuuspaketti (Composed Assurance Package, CAP). Se keskittyy komponenttien yhteentoimivuuden turvallisuuden arviointiin (*ISO/IEC 15408-3:2008* 2008, pykälä 8.1). Se olettaa, että osaset on arvioitu

itsenäisesti ja antaa kolmiportaisen asteikon, josta voi valita tarpeen mukaan kevyimmän CAP-A:n tai kaikkein tarkimman CAP-C:n.

ISO/IEC 15408 -standardisarja formalisoi turvallisuuden testausta lähtien siitä, miten yleisempiä turvallisuusvaatimuksia jaotellaan ja ilmoitetaan puolustusprofiileihin tuoteryhmälle yhteiseksi ja turvatavoitteiksi, yksittäiselle kohteelle. Toinen osa standardista käy läpi tarkemmin turvavaatimuksia antaen joukon valmiita, käytettäviä vaatimuksia. Kolmas osa keskittyy näiden arviointiin ja testaamiseen antaen yksittäisiä vakuutusvaatimuksia ja niiden hierarkisia rakenteita sekä valmiita paketteja eri turvallisuuden tarpeille yksittäisille tutkimuksenkohteille, että usean osan kokoonpanon analysointiin.

6 Lääkintälaitteiden turvallisuusstandardeja

Lääkintälaitteiden standardeja ja määräyksiä on laaja kirjo, joka vaihtelee maakohtaisesti (Ståhlberg 2015, s. 15). Suomessa keskeisintä on CE-merkinnän saaminen, joka edellyttää Euroopan Unionin määräyksien seuraamista (Ståhlberg 2015). Ståhlbergin (2015, s. 20) mukaan CE-merkinnällä on merkitystä myös EU:n ulkopuolelle siirryttäessä, sillä jotkin maat vaativat omien määräyksiensä noudattamisen lisäksi vientitodistusta (Free Sales Certificate).

EU-tasolla vaikuttaa Euroopan neuvoston direktiivi 93/42/ETY (annettu 14. päivänä kesäkuuta 1993) lääkinnällisistä laitteista, jäljempänä lääkintälaitedirektiivi. Lääkintälaitteiden CE-merkinnän saaminen edellyttää lääkintälaitedirektiivin vaatimusten täyttymistä (*Lääkintälaitedirektiivi* 1993, 17 artiklan kohta 1). Turvallisuuden näkökulmasta lääkintälaitteet jaotellaan luokkiin niihin liittyvien riskien mukaan, ja luokan perusteella laitten "vaatimustenmukaisuuden arviointimenettelyt" eroavat (*Lääkintälaitedirektiivi* 1993, s. 86). Direktiivin luokka I on riskittömin ja sen arvioi pääosin valmistaja itse. Luokan II kohdalla ilmoitetun laitoksen on tarkistettava laite. Ilmoitettu laitos on laitos, jonka valtio on valinnut tarkistamaan kyseisiä vaatimuksenmukaisuuksia (*Lääkintälaitedirektiivi* 1993, 16 artiklan kohta 1); esimerkiksi Suomessa tällainen laitos on VTT Expert Services Oy. Luokalle IIa riittää ilmoitetun laitoksen tarkistus valmistusvaiheessa, kun taas IIb ja III tarvitsevat tarkistuksen myös suunnitteluvaiheessa (*Lääkintälaitedirektiivi* 1993, s. 86). Luokka III sisältää vaarallisimmat laitteet, jotka vaativat erillisen ennakkoluvan (*Lääkintälaitedirektiivi* 1993, s. 86).

Maailmanlaajuisella tasolla vaikuttaa ISO. Se kehittää standardeja aihealueisiin erikoistuneiden teknisten komiteoiden avulla. Terveydenhuoltoon liittyvän tietotekniikan standardoinnin tekninen komitea on numeroltaan 215 ja nimeltään "Health Informatics". Sen tarkoituksena on edistää laitteiden ja järjestelmien yhteentoimivuutta sekä vähentää turhaa ja päällekkäistä vaivaa (*ISO/TC 215 Business Plan* 2013). Vaikka sen ydinaiheena ei ole turvallisuuden kehittäminen, on sillä siihen erikoistunut työryhmä ISO/TC 215/WG 4 "Safety, Security and Privacy", eli turvallisuuden ja yksityisyyden työryhmä.

Lääkintälaitteiden kyberturvallisuuteen liittyviä ISO-standardeja ovat mm.

- ISO/IEC 27001:2013 Information technology – Security techniques – Information

security management systems – Requirements

- ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls
- ISO/IEC 27799:2008 Health informatics – Information security management in health using ISO/IEC 27002
- ISO/TS 13606-4:2009 Health informatics – Electronic health record communication – Part 4: Security
- ISO/TR 11633-1:2009 Health informatics – Information security management for remote maintenance of medical devices and medical information systems – Part 1: Requirements and risk analysis
- ISO/TR 21730:2007 Health informatics – Use of mobile wireless communication and computing technology in healthcare facilities – Recommendations for electromagnetic compatibility (management of unintentional electromagnetic interference) with medical devices
- ISO/TR 21089:2004 Health informatics – Trusted end-to-end information flows

Lisäksi on kaksi standardisarjaa ISO/IEEE 11073 ja IEC/TR 80001, jotka koskettavat aihetta. ISO/IEEE 11073-sarja on tarkoitettu monien lääkintälaitteiden kommunikointitapojen määrittelyyn, nimenään “Health informatics – Point-of-care medical device communication”. IEC/TR 80001-sarja ("Application of risk management for IT-networks incorporating medical devices") keskittyy lääkintälaitteita sisältävän tietoverkon riskien hallintaan.

Anita Finnegan ja Fergal McCaffery (2015) keräsivät suosituksia asiantuntijoilta ja päätyivät nojaamaan työssään seuraaviin standardeihin neljän asiantuntijan suosituksesta: ISO/IEC 27001 (Information technology – Security techniques – Information security management systems – Requirements), ISO 27799 (Health informatics – Information security management in health using ISO/IEC 27002), ISO/IEC 15408-2 (Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components) , ISO/IEC 15408-3 (Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components), NIST 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations), IEC 62443-3-3 (Industrial communication networks - Network and system security - Part 3-3: System security require-

ments and security levels). Lisäksi heidän työnsä pohjalta kehitettiin uusia teknisiä raportteja: IEC/TR 80001-2-9 ja IEC/TR 80001-2-8.

Tässä työssä pohjataan erityisesti seuraaviin standardeihin ja teknisiin raportteihin :

- ISO/IEC 15408-1:2009 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model
- ISO/IEC 15408-2:2008 Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components
- ISO/IEC 15408-3:2008 Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components
- IEC/TR 80001-2-2:2012 Application of risk management for IT-networks incorporating medical devices – Part 2-2: Guidance for the communication of medical device security needs, risks and controls
- IEC/TR 80001-2-3:2012 Application of risk management for IT-networks incorporating medical devices – Part 2-3: Guidance for wireless networks

6.1 IEC/TR 80001

IEC/TR 80001 -standardisarja ohjeistaa lääkintälaitteita sisältävän verkon riskienhallintaan. Standardisarjassa on useita osia: mm. IEC 80001-1:2010 määrittelee roolit, vastuut ja toimet, IEC/TR 80001-2-2:2012 ohjaa turvallisuuden osa-alueiden termeihin ja niistä viestintään ja IEC/TR 80001-2-3:2012 ohjeistaa langattomien verkkojen käyttöön. Tässä työssä käsitellään IEC/TR 80001-2-2 ja IEC/TR 80001-2-3, eli yleisesti turvallisuuden parantamisen soveltamisesta ja tarkemmin langattomien verkkojen yhteydessä.

IEC/TR 80001 ei ole tyhjiössä. Sen termit ovat lähellä ISO 14971 -standardia ja näitä eroja käydään läpi IEC/TR 80001-2-2:ssa (*IEC/TR 80001-2-2:2012* 2012, pykälä 4.3). Se on mainin-nut samoja turvatoimia kuin ISO 15408-2. Automaattinen uloskirjautuminen toimettomuuden jälkeen on standardeille yhteinen. ISO 15408-2:ssa se on määritelty turvallisuuskomponentti koodiltaan FTA_SSL.1 ja lääkintälaitestandardissa se on koodillaan ALOF (*IEC/TR 80001-2-2:2012* 2012, pykälä 5.1). Listattuna on myös lääkintälaitteille erityisiä toimintoja, kuten pääsyn antaminen hoitohenkilökunnalle hätätilanteissa (koodina EMRG) (*IEC/TR 80001-2-*

2:2012 2012, pykälä 5.8). Tähän hätätilanteiden erityisyyteen perehdytään enemmän luvussa 4.2.3.

IEC/TR 80001-2-2:2012 keskittyy kommunikaation parantamiseen. Se listaa turvaominaisuuksia (security capabilities), jotka voidaan nähdä turvavaatimuksina, esimerkiksi automaattinen uloskirjautuminen ja datan varmuuskopiointi. Näiden tarkoituksena on helpottaa velvollisuuksista keskustelua eri osapuolten välillä (*IEC/TR 80001-2-2:2012* 2012, pykälä 4.1). Liitteessä A annetaan yksinkertaistettu esimerkki siitä, miten näitä voidaan hyödyntää keskustelussa esimerkiksi sairaalan ja laitevalmistajan välillä. Eri standardien vaatimukset eroavat eri alueilla ja siihenkin on annettu esimerkki liitteessä B. Monissa turvaominaisuuksissa kerrotaan, mistä tämä vaatimus on peräisin, ja soveltamista voidaan tehdä keskittymällä oman alueen viranomaisten vaatimuksiin.

6.2 IEC 60601

IEC 60601 -sarja sisältää monia lääkintälaitteiden turvallisuuteen liittyviä standardeja, mukaan lukien hälytyksille ja niiden äänille (IEC 60601-1-8:2006) sekä kotisairaanhoidon laitteiden turvallisuudelle (IEC 60601-1-11:2015). IEC 60601 -sarja käsittelee keskeisiä vaatimuksia turvallisuuden ja toimivuuden suhteen. Standardit voidaan jaotella yleisiin ja laitetyyppiin liittyviin. Yleisten ominaisuuksien kuvaukset koskevat esimerkiksi käytettävyyttä (IEC 60601-1-6) ja ympäristöystävällistä suunnittelua (IEC 60601-1-9). Laitetyyppiin liittyvät määrittelevät lukuisille laitteille niiden vaatimukset, mm. röntgenlaitteille (IEC 60601-1-3) ja keskoskaapeille (IEC 60601-2-19).

7 Laitteen testaaminen

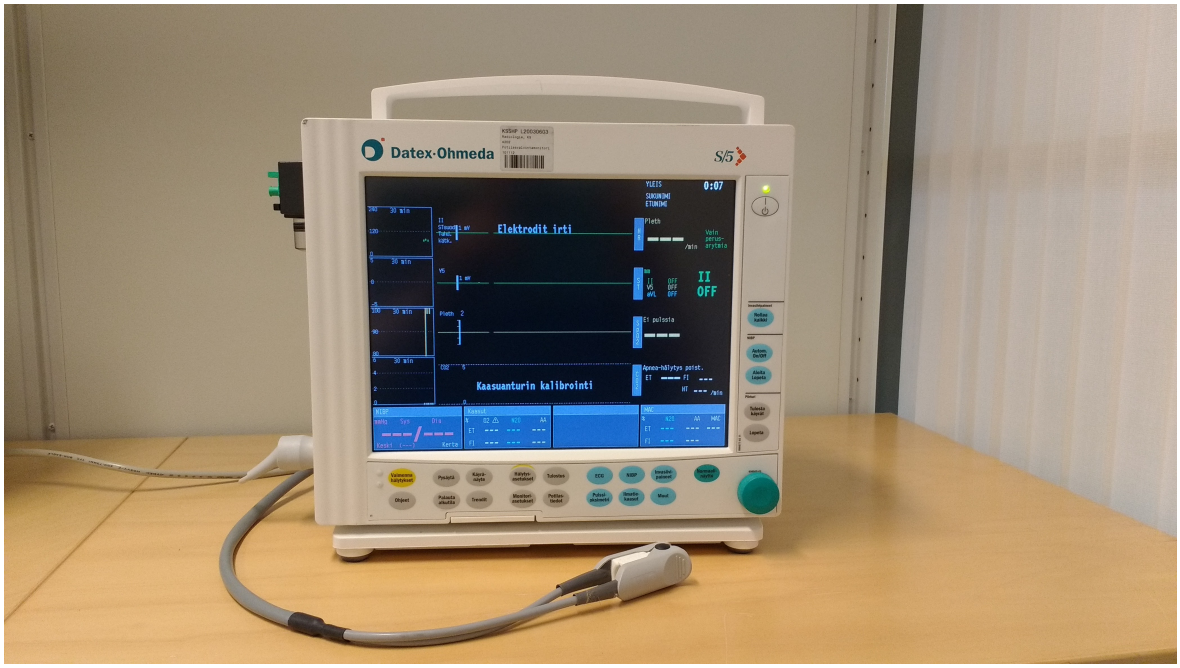
Määritellään tässä tutkielmassa käytettyä testaamista luvun 3.4 testauksen jaottelun mukaan. Tämä testaaminen oli mustalaatikkotestaamista, sillä testeissä ei käytetty tietoa laitteen sisäisestä rakenteesta. Lisäksi se oli järjetelmätestausta, sillä koko laite oli testattavana. Tarkoituksen puolesta tämä testi kuuluu osoitusmalliin, jossa verrataan laitetta ulkopuolelta tulleisiin vaatimuksiin. Testaustekniikka oli yhdistelevää. Testattavat ominaisuudet testeille, esimerkiksi potilastietojen eheyden säilyminen, poimittiin määrityksistä, kun taas varsinainen asian testaus nojasi testaajan intuitioon. Lisäksi testaus oli ad hoc -tyylistä, perustuen kokeiluun. Kokeiltiin siis, millä tavoin testivaatimuksia voitaisiin rikkoa.

7.1 Tutkittava laite

Laite on Datex-Ohmedan S/5 anestesiamonitori, joka otettiin käyttöön Keski-Suomen sairaanhoitopiirissä (KSSHP) vuonna 2003 ja poistettiin hiljattain käytöstä. Laitteen käyttöliittymä on suomeksi ja laite sisältää ohjevalikon, ks. kuvio 2. Käyttöohjeita löytyi Internetistä, kun kirjautui MedWrench-sivustolle (*Datex Ohmeda - S/5 Compact Community, Manuals, Specifications : MedWrench* 2017). MedWrench on lääkintälaitteiden käyttäjien verkostoitumis- ja tiedonsaantisivusto; sieltä löytyy keskusteluita laitteiden käytöstä ja ohjekirjoja ladattavaksi. Ohjekirja viittaa standardeista 60601-1-1 standardiin, muistuttaen mm. että monitoria liitettäessä muihin laitteisiin myös yhdistelmän tulee noudattaa kyseistä standardia (*Document no. M1031517-02* 2006, s. 31).

Monitori kuuluu EU:n lääkintälaitedirektiivin luokkaan IIb (*Document no. M1031517-02* 2006). Luokitus kertoo kuinka tiukasti laitteen suunnittelua ja valmistusta on seurattu direktiivin vaatimusten noudattamisen suhteen. Laitteen luokitus perustuu siihen, kuinka paljon haittaa laite voi aiheuttaa väärin toimiessaan ihmisruumiille (*Lääkintälaitedirektiivi* 1993, s. 86). IIb luokka on toiseksi tiukin luokka: ulkopuolisen laitoksen tulee tarkistaa vaatimustenmukaisuus sekä suunnittelu- että valmistusvaiheelle (*Lääkintälaitedirektiivi* 1993, s. 86).

Laitetta voidaan muokata erilaisilla moduuleilla. Muun muassa happisaturaation, EKG:n



Kuvio 2. Tutkittava potilasmonitori on Datex-Ohmedan S/5 anestesiamonitori. Kuvassa on monitorin lisäksi veren happisaturaation sormesta mittaava moduuli.

ja verenpaineen sekä kaasumoduuli löytyvät. Tässä tilanteessa on mahdollisuus käyttää happisaturaatiota ja verenpainetta. Puuttuvia moduuleita ovat esimerkiksi muistikortti- ja tulostusmoduuli.

7.1.1 Tietoliikenneyhteydet

Laitteeseen voi saada tietoliikenneyhteyden neljää kautta: LAN, WLAN, sarjaportti sekä ohjelmointikytkentä, joka näyttää sarjaportilta. Lisäksi yhteyksiä muihin lääkintälaitteisiin voitaisiin lisätä yhteysmoduuleilla (E-INT / M-INT ja laitekohtaiset N-DISxxx moduulit) (*Document no. M1031517-02* 2006, s. 31).

Laitteessa on Ethernet-portti. Kun monitori kytketään Ethernet-kaapelilla tietokoneeseen, huoltovalikossa näkyy laitteen tilan muutos: se on yhteydessä LAN-verkkoon.

WLAN-yhteys tarvitsee WLAN-PC-kortin (*Document no. M1031517-02* 2006, s. 18) ja sitä ei tässä tapauksessa ole käytössä. Monitori voi salata langattoman liikenteen WEP-salauksella (*Document no. M1031517-02* 2006, s. 9). WEP on haavoittuvaksi havaittu menetelmä, mutta

laite on vanha, mikä selittänee tämän puutteen.

Monitori voidaan kytkeä valmistajan Datex-Ohmeda verkkoon langallisesti tai langattomasti. Tämä verkko rakentuu TCP/IP:n päälle ja sen hubit ovat moniporttisia toistimia (*Document No. 8000633-1* 2000, s. 5 ja 3). Hubin kautta monitorit ovat yhteydessä keskukseen, jolle ilmoitetaan monitorien lukumäärä erillisen avaimen avulla (*Document No. 8000633-1* 2000, s. 5 ja 3). Tällä tavalla huomataan ylimääräisten monitorien liittymisyritykset sekä monitorien tippumiset verkosta.

Sarjaportti on tarkoitettu lasertulostinta ja tietokonetta varten (*Document no. M1031517-02* 2006, s. 42 ja 44). Tulostimen liittäminen ei vaadi juurikaan valmisteluja, ja laite syöttää portista dataa, vaikka vastassa olisi tietokone. Laitteen tietokonerajapinnan tietoja ei ole annettuna saatavilla olevissa ohjeissa, vaan niissä kehotetaan ottamaan jälleenmyyjään yhteyttä (*Document no. M1031517-02* 2006, s. 44).

Monitorissa on ohjelmointikytkentä. Se on sarjaportin näköinen portti, joka kuitenkin eroaa kytkennöiltään sarjaportista. Portti sisältää mm. hoitajan kutsumiselle omistetun pinnin ja useat viestien kululle oleelliset pinnit ovat eri kohdassa kuin sarjaportissa. Tämä kytkentä on todennäköisimmin valmistajan oma, joten sen käyttöön ei ulkopuolisia ohjeita juuri löydy.

7.1.2 Käyttö

Laitteen hoitoon liittyviä ominaisuuksia pystytään muuttamaan, kun päästään käsiksi näppäimiin. Kaikkeen ei tie ole avoinna: Asennus/Huolto-valikko on salasanasuojattu. Salasana on oletettavasti kolmen luvun yhdistelmä. Luvut ovat kokonaislukuja välillä 1 - 100 ja niitä käydään läpi rullaa pyörittämällä. Kolmen väärän luvun syöttämisen jälkeen laite palaa edelliseen valikkoon. Salasanat löytyvät teknisestä huolto-ohjekirjasta, joka on ladattavissa Internetistä (*Document no. M1031517-02* 2006, s. 2).

Laite soittaa hälytysääniä mm. matalan happisaturaation (SP02) vuoksi. Hälytysäänet otettiin pois käytöstä, joskin valinta ei säily uudelleenkäynnistyksen yli.

7.2 Metodi

Ensin tutustuttiin laitteeseen ja sen yhteyksiin. Sen jälkeen tarkasteltiin standardeja ja poimittiin niistä vaatimuksia, jotka ovat oleellisia ja testattavissa laitteesta. Sitten tutkitaan, toteuttaako laite nämä vaatimukset.

Potilasmonitoreille ei ole julkisia suojausprofiileja tai turvatavoitteita. Lääkintätiedon käsittelyyn tarkoitetuille ohjelmille on suojausprofiili Common Criterian sivuilla, mutta se ei koske monitoria. Tämän puutteen takia kootaan ISO 80001-2-2:sta löytyvistä vaatimuksista laitteeseen sopivia turvaominaisuuksia yhteen ja testataan näitä vaatimuksia.

7.3 Laitteesta tutkittavat vaatimukset

Tässä osiossa käydään läpi, mitä vaatimuksia valittiin testattavaksi. Sen jälkeen perustellaan, miksi joitain jätettiin pois. Englanninkieliset nimet ja lyhenteet ovat raportin käyttämiä.

7.3.1 Tutkittavat vaatimukset

Automatic logoff – ALOF: Automaattinen uloskirjautuminen estää asiattomien pääsyn laitteen asetuksiin ja tietoihin (*IEC/TR 80001-2-2:2012* 2012, pykälä 5.1). Laitteessa on kahden tasoisia salasanasuojattuja valikoita. Tutkitaan, poistuuko laite näistä valikoista kahdessatoista tunnissa, jos laitetta ei käytetä.

Authorization – AUTH: Turvallisena periaatteena olisi rajoittaa potilastietoihin ja laitteen toimintoihin pääsy vain heille, jotka sitä tarvitsevat (*IEC/TR 80001-2-2:2012* 2012, pykälä 5.3). Tarkistetaan, vaatiiko potilastietojen tarkastelu ja laitteen toimintojen käyttö tunnistautumista.

Health data de-identification – DIDT: Potilaan tiedot tulee voida poistaa järjestelmästä tai ainakin poistaa tunnistettavat tiedot (*IEC/TR 80001-2-2:2012* 2012, pykälä 5.6). Tutkitaan, voiko näin tehdä.

Emergency access – EMRG: Jotta hätätilanteessa laite on käytettävissä, on hyvä olla mekanismi, jolla laitteen tietoihin ja toimintoihin pääsee käsiksi kirjautumatta sisään henkilöille myönnetyillä tunnuksilla (*IEC/TR 80001-2-2:2012* 2012, pykälä 5.8). Tutkin, voiko laitteen

olennaisimpia toimintoja käyttää ilman salasanoja ja muita tunnistautumisia.

Health data integrity and authenticity – IGAU: Potilaan tietojen tulisi olla oikein ja saatavilla (*IEC/TR 80001-2-2:2012* 2012, pykälä 5.9). Tutkitaan, löytyykö yksinkertaisia tapoja peukaloida tietoja.

System and application hardening – SAHD: Koventamisella tarkoitetaan hyökkäysvektorien karsimista niin vähiin kuin mahdollista mahdollistaen silti "oleelliset toiminnot" (*IEC/TR 80001-2-2:2012* 2012, pykälä 5.15). Arvioidaan, onko järjestelmässä tarpeettomia aukkoja.

Health data storage confidentiality – STCF: Tallennetun potilastiedon tulee olla ehyttä ja luottamuksellista (*IEC/TR 80001-2-2:2012* 2012, pykälä 5.17). Tutkitaan, kuinka vaikeaa on saada tiedot haltuun ja muuttaa niitä.

Transmission confidentiality – TXCF: Lähetetyn datan luottamuksellisuus. *IEC/TR 80001-2-2:2012* (2012, pykälä 5.18) nojaa paikallisiin lakeihin. EU-alueella olennaisessa osassa on Euroopan parlamentin ja neuvoston direktiivi 95/46/EY (annettu 24 päivänä lokakuuta 1995), yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta.

Transmission integrity – TXIG: Tutkitaan, miten lähetetyn datan eheyttä edistetään.

7.3.2 Pois jätettävät vaatimukset

IEC/TR 80001-2-2 sisältää muitakin vaatimuksia, mutta ne jätetään tämän tutkielman ulkopuolelle. Kaikki turvaominaisuudet eivät ole oleellisia kaikille laitteille (*IEC/TR 80001-2-2:2012* 2012, pykälä 4.2). Vaatimuksia karsittiin myös testauskyvyn vajavaisuuksien vuoksi. Laitetta tutkittiin mustana laatikkona: ilman sisäpiirin tietoa sen toiminnasta tai etukäteen saatua pääsyä sen järjestelmään. Tämän vuoksi esimerkiksi moninaisten lokien olemassaoloa tai sisältöä ei voitu tutkia ilman pääsyä järjestelmän sisälle. Toisekseen, jotkin eivät olleet olennaisia tämän tukielman näkökulman kannalta. Esimerkiksi laitteen fyysinen turvallisuus tai elinkaaren turvallisuuden tutkiminen jätettiin ulkopuolelle.

8 Tulokset

Oleellisin tulos oli, että fyysisen käyttöliittymän kautta laite on hyvin avoin. Se antaa käyttää laitetta sekä kirjata ja muokata potilastietoja. Tämän myötä suurin osa luottamuksellisuuteen ja eheyteen liittyvistä vaatimuksista jäivät täyttymättä. Potilastietojen poistaminen onnistui laitteelta, mikä estää luottamuksellisten terveystietojen päätymistä vääriin käsiin. Tietoliikenneyhteyksien kautta laitteeseen ei juurikaan saatu kontaktia, ainoastaan fyysisen käytöliittymän kautta aloitettu tulostus paljasti potilastietoja ja mahdollisti järjestelmän kaatamisen.

Aluksi tutkittiin Ethernet- ja sarjaportteja ja yritettiin saada niiden kautta yhteys laitteeseen tai ainakin poimia monitorin lähettämiä viestejä. Ethernet-portin kuunteleminen ei paljastanut mitään. Kuunteleva tietokone lähetti paljon viestejä, mutta monitorista ei kuulunut mitään. Kun monitori liitettiin tavalliseen reitittimeen, ei monitori reagoinut muuten kuin näyttämällä oman näyttönsä asetuksissa olevansa kiinni Ethernet-verkossa. Monitori ei kuitenkaan näkynyt reitittimen asiakaslistauksessa.

Luultavasti laite vaatisi, että käytettäisiin valmistajan protokollaa, jolla monitorit keskustelevat keskuslaitteen kanssa. Tämän protokollan tietoja ei löytynyt ohjekirjasta, muuta kuin että pohjana on Ethernet, mutta pakettien sisältö on valmistajan omaa (*Document No. 8000633-1* 2000, s. 9). Lisäsyynä liittymättömyyteen voi olla se, että sille ei annettu osoitetta ohjelmointikytkennän kautta (*Document No. 8000633-1* 2000, s. 15). Tämä olisi vaatinut uudenlaisen liittimen tekemistä ja protokollan selvittämistä.

Sarjaportista saatiin ulos tulostimelle tarkoitettuja viestejä. Sarjakaapeli yhdistettiin Windows-pöytäkoneen sarjaporttiin ja otettiin yhteys Windowsin Kitty-ohjelmaan. Data on tarkoitettu lasertulostimelle, joten siinä ei juuri ole selvätekstistä viestiä.

Kun sarjaporttia yritettiin käsitellä Linux Ubuntu koneen terminaalilla, tulostaminen aiheutti potilasmonitorin kaatumisen. Tässä käytetyt komennot olivat: ‘sudo stty -F /dev/ttyS0 115200’ ja ‘sudo hexdump -C /dev/ttyS0’ tai jälkimmäisessä käy myös ‘sudo cat /dev/ttyS0’. Eli huonosti käyttäytyvä tulostin saa monitorin käynnistymään uudelleen, jos monitorilla yritetään tulostaa. Kun sarjaportti välitettiin virtuaalikoneessa olevaan Linux Ubuntu -koneeseen ja

käytettiin Cutecom-ohjelmaa, tulostus oli samanlaista tekstiä kuin Windowsin Kittyllä.

8.1 Vaatimusten testauksen tulokset

Seuraavaksi käydään läpi jokaisen vaatimuksen testauksen tulokset. Tässä testataan, toteuttaako monitori ISO:n teknisen raportin 80001-2-2 vaatimuksia, joista karsittiin osa pois osiossa 7.3.2. Tulokset on jaoteltu raportin vaatimusten mukaan, sisältäen raportissa esiintyvän nimen ja lyhenteen.

Automatic logoff – ALOF: Suojatuista valikoista uloskirjautuminen käyttämättömyyden myötä suojaisi asetuksien luvatonta muuttamista. Vaadittiin siis automaattista uloskirjautumista. Laitteeseen kirjauduttiin työpäivän päätteeksi ensin syvimpään, kahden salasanan takaiseen valikkoon ja toisena päivänä yhden salasanan takaiseen valikkoon. Aamulla tarkistettiin, oliko laite poistunut salasanoja vaativasta valikosta. Se ei tehnyt sitä kummassakaan tilanteessa, vaan odotti yli kahdentoista tunnin jälkeen samassa valikossa, kuin mihin se jätettiin. Ensimmäisellä testikerralla vaikutti siltä, että laite olisi kirjautunut ulos, sillä se oli palannut alkunäkymään. Laite oli kuitenkin käynnistynyt jostain syystä uudelleen, mikä näkyi siinä, että syötetyt potilastiedot olivat nollautuneet. Tämän epäilyn vuoksi koe toistettiin ja monitori ei kirjautunut ulos. Monitori ei siis täyttänyt vaatimusta.

Authorization – AUTH: Tarkistettiin, vaatiiko potilastietojen tarkastelu ja laitteen toimintojen käyttö tunnistautumista. Potilaan tietoihin pääsi käsiksi ilman salasanaa käyttäen monitorin näppäimiä ja valintarullaa. Tiedot sisältivät mm. nimen, henkilöturvatunnuksen, painon ja pituuden sekä näytteiden tuloksia. Tätä vaatimusta monitori ei täytä.

Health data de-identification – DIDT: Vaatimus on, että potilaan tiedot tulee voida poistaa järjestelmästä tai ainakin poistaa tunnistettavat tiedot (*IEC/TR 80001-2-2:2012* 2012, pykälä 5.6). Uudelleenkäynnistäminen tyhjensi potilaan tiedot monitorin muistista tai ainakaan niitä ei saa monitorin valikoita selaamalla näkyviin. Tämä vaatimus täytetään.

Emergency access – EMRG: Vaatimuksena on, että laitteen olennaisimpia toimintoja voidaan käyttää ilman salasanoja ja muita tunnistautumisia fyysisen käyttöliittymän kautta. Salasanoja tarvittiin asetusten muuttamiseen, mutta potilaan elintoimintoja pystyi seuraamaan ilman

kirjautumista. Myös potilaan henkilötietoja ja laboratoriotuloksia pystyi selaamaan, lisäämään ja muokkaamaan ilman tunnistautumista. Hätätilanteen käytön kannalta tämä potilasmonitori on toimiva ja vaatimus täytetään.

Health data integrity and authenticity – IGAU: Potilaan tietojen tulisi olla oikein ja muuttumattomia. Tätä tutkittiin testaamalla, löytyykö yksinkertaisia tapoja peukaloida tietoja. Potilaan tietojen peukalointi näytöltä oli hyvin helppoa, minkäänlaista salasanaa ei tarvittu. Tämä koski sekä henkilötietoja että laboratoriotuloksia. Laboratoriotuloksia varten täyti valita syöttömuodoksi manuaalinen, jotta laboratoriotuloksia voi lisätä käsin. Tuloksille voi asettaa näytteenottoajan, joten menneisyyteen voi syöttää vääriä arvoja. Manuaalista syöttötapaa ei näy vanhoissa näytetiedoissa, joten luotettavuutta on vaikea todentaa. Lisäksi vanhoja näytteiden arvoja voidaan muokata jälkikäteen. Tästä tosin jää merkintä: *-merkki tulee muutetun arvon viereen. Eheys ei siis ole taattua. Vaatimusta ei täytetä.

System and application hardening – SAHD: Tutkitaan, onko järjestelmä kovennettu, eli onko tarpeettomat aukot poistettu. Ethernet-kaapelin kautta ei saatu mitään yhteyttä, sillä laite ei neuvottele itselleen IP-osoitetta, kun se kytketään tietokoneeseen tai reittimeen. Lisäksi ohjelmointikytkentä ei ole sarjakytkentästandardien mukainen, vaan sen käyttö vaatii oman kaapelin tekemistä ja protokollan ymmärtämistä. Nämä reitit ovat kuitenkin käytettävissä kun oikea protokolla on tiedossa. Kovennus vaatii *tarpeettomien* yhteyksien poistamista eikä ilman tarkempia tietoja voida sanoa, ovatko nämä väylät tai niissä sallitut viestit minimoitu. Vaatimuksen täyttymisestä ei voida olla varmoja.

Health data storage confidentiality – STCF: Tallennetun potilastiedon tulee olla ehyttä ja luottamuksellista. Potilaan nimen, henkilöturvatunnuksen, painon ja pituuden pystyi muuttamaan, jos pääsi monitorin näppäimiin käsiksi. Tästä muuttamisesta ei jäänyt monitorin näytöltä havaittavia jälkiä. Eheys ja luottamuksellisuus eivät siis olleet taattuja, jos laitteeseen oli fyysinen pääsy. Vaatimusta ei täyty.

Transmission confidentiality – TXCF: Lähetetyn datan tulisi pysyä luottamuksellisena. Tulostimelle lähetettävässä datassa on potilaan nimi ja henkilöturvatunnus, jos ne on kirjattu monitoriin. Nämä tiedot ovat selkotekstinä, eli ne ovat suoraan luettavissa, ilman salausta. Lähetys ei siis ole luottamuksellinen.

Transmission integrity – TXIG: Ohjeen mukaan lähetetyn datan eheyttä edistetään CRC:n käytöllä (*Document No. 8000633-1* 2000, s. 9). Tätä ei kuitenkaan voitu testata käytännössä, sillä laitteen käyttämä protokolla ei ollut tiedossa ja mitään viestejä ei saatu laitteen Ethernet-portin kautta. Vaatimuksen täyttymisestä ei voida tehdä johtopäätöksiä.

9 Johtopäätökset

Tässä tutkielmassa käytiin läpi lääkintälaitteiden kyberturvallisuuteen liittyvää kirjallisuutta ja standardeja. Tarkoituksena oli kytkeä kyberturvallisuusstandardit käytäntöön testaamalla yhtä lääkintälaitetta niiden suosituksia vasten. Tässä kappaleessa poimitaan oleellisimpia tuloksia ja pohditaan tulosten vaikutuksia käytäntöön ja mahdollisia tutkimussuuntia.

9.1 Testauksen tulokset

Käytännön osuudessa tutkittiin, noudattaako potilasmonitori ISO 80001-2-2 raportissa esitettyjä turvaominaisuuksia. Fyysisen käyttöliittymän kautta laite oli hyvin avoin. Sitä pystytiin käyttämään kirjautumatta; ainoastaan osa asetuksista oli salasanojen takana. Avoimuus on hyvä puoli hätätilanteiden varalle, mutta potilastietojen luottamuksellisuus on kovalla koitoksella tässä laitteessa.

Tietoja pystytään katsomaan ja luomaan ilman kirjautumista eikä siitä jää havaittavaa jälkeä. Laboratoriotulosten muuttaminen jättää merkin muutetun tiedon viereen, mikä paljastaa mahdollisen väärennöksen. Laite on avoin näytön ja näppäimistön kautta, ja näiden pitkäaikainen käyttäminen saattaisi herättää epäilyksiä. Tietojen syöttäminen ei ole nopeaa tai kätevää, joten väärennettyjen laboratoriotulosten syöttämisessä todennäköisesti vierähtäisi tovi, mikä lisää kiinnijäämisen riskiä.

Tutkittuun monitoriin ei juuri päästy käsiksi sen tietoliikenneporttien kautta. Ethernet-portissa käytössä on valmistajan oma protokolla eikä sieltä saatu minkäänlaista yhteyttä. Tämä antaa lisäesteen laitteen hakkeroinnille. IP-verkkojen kautta hyökkäämiseen on monia työkaluja ja se, että laite ei automaattisesti liity Ethernet-portin kautta antaa hyökkääjille pienen lisähaasteen. Tällöin hyökkääjien tapa hankkia laite ja kartoittaa sen heikkouksien omassa rauhassa (Laszka, Felegyhazi ja Buttyan 2014, s. 23:3) vaikeutuu hieman, kun laitteeseen ei saa heti kontaktia. Tosin protokollan tuntemattomuus ei loputtomasti suojele, sillä tuntemattomuuden turva ei ole kestävä suoja (ks. luvusta 3.3).

Ainoastaan tulostaminen sarjaportin kautta paljasti potilastietoja, mutta sekin vaati monitorin

fyysisten painikkeiden käyttöä. Tulostamisen aikana monitorin sai kaadettua. Laite kaatui, kun se tulosti alustamattomaan tietokoneen sarjaporttiin. Monitorin uudelleenkäynnistyminen voi haitata hoitoa, sillä monet monitorin asetuksista eivät säily uudelleenkäynnistyksen yli. Potilaan tiedot mm. nimi ja paino katoavat ja hälytysten asetukset palautuvat oletustilaan sekä aika nollautuu vuoteen 1995 tammikuun ensimmäiseen päivään.

Monitori ei myöskään lähetä viestejä sarjaportin kautta paitsi tulostettaessa. Se ei siis anna vihjeitä oikean protokollan löytämiseen. Yhteys tietokoneeseen lienee mahdollista ainakin joissain malleissa, sillä ohjekirjan mukaan ohjeistuksia yhteyden muodostamiseen tulee kysyä jälleenmyyjältä (*Document no. M1031517-02* 2006, s. 44). Näiden reittien tarpeellisuudesta tai tarpeettomuudesta on vaikea todeta mitään ilman tarkempia tietoja valmistajalta. Jos ei tiedetä tarkkaan, mitkä ovat tämän laitteen oleelliset toimet, ei voida päätellä onko kaikki muu estetty. Tämän takia ei voida päätellä, täyttyykö kovennusta vaativa turvaominaisuus.

Ainut tieto lähetysten eheydestä oli ohjekirjassa, jonka mukaan monitori käyttää CRC:tä (*Document No. 8000633-1* 2000, s. 9). CRC auttaa toki viestiliikenteen kohinaa vastaan, mutta tahallista manipulointia se ei estä (Stigge ym. 2006, s. 17; Peris-Lopez ym. 2009, s. 374). Saattaa olla, että valmistajan verkon protokollassa on eheyden varmistavia menetelmiä, esimerkiksi salauksia. Näistä ei kuitenkaan ole tietoa, sillä yhteyttä laitteeseen ei saatu Ethernet-portin kautta.

IEC/TR 80001-2-2 -raportti suosittelee uloskirjautumista, mutta voi olla, että laitetta tehdessä ollaan todettu, ettei tätä ominaisuutta tarvita tai että kirjaudutaan ulos viikon kuluttua. Tämän tutkimus testasi, kirjautuiko laite ulos kahdentoista tunnin kuluessa. Toiseksi, henkilötietoja oli selkotekstinä tulostimelle lähetettävässä datassa. Tämä kuulostaa tiedustelureitiltä. Sen pohjalta ei kuitenkaan voida päätellä, onko monitori kovennettu huonosti. Ilman monitorin ja tulostimen tarkempia teknisiä tietoja on mahdotonta sanoa, ovatko nämä tiedot datassa tarpeellisia vai tarpeettomia.

Lisäksi tiedustelureittinä tulostuksen kaappaaminen olisi työläs. Se vaatisi hyökkääjältä fyysistä paikalla oloa, oman laitteen kytkemistä sarjaporttiin ja tulostuksen aloittamisen monitorin näppäimillä. Lisäksi kun laite tulostaa useita sekunteja, näkyy näytössä “Tulostaa...”-ilmoitus, mikä lisää kiinnijäämisen riskiä.

Standardien noudattamisen mustalaatikkotestaaminen on hankalaa, sillä monien kohtien tarkistaminen vaatii tarkkaa tietoa siitä, mitä laitteen on suunniteltu tekevän. Esimerkiksi automaattinen uloskirjautuminen ja koventaminen ovat tämän tyyppisiä suosituksia ISO 80001-2-2 -raportissa. Lisäksi varmistamista vaatisi se, että riittääkö tälle laitteelle viestien eheyden varjeleminen kohinaa vastaan, vai olisiko tahallistakin häiriötä ja manipulointia vastaan suojauduttava. Näihin kaikkiin liittyy mahdollinen haavoittuvuus tai suositusten noudattamattomuus, mutta ilman laitteen valmistuksen tarkkoja suunnitelmia ei voida tehdä varmoja johtopäätöksiä. Näiden tulosten pohjalta voidaan todeta, että tämän potilasmonitorin turvallisuus nojautuu pitkälti sen fyysisen ympäristön turvallisuuteen. Tästä johtuen pääsyä käytössä olevaan monitoriin tulisi rajoittaa, jotta potilaan tiedot eivät joutuisi vääriin käsiin. Toinen vaihtoehto olisi säilyttää laitteessa mahdollisimman vähän tietoa, jolloin sen joutuminen vääriin käsiin aiheuttaisi mahdollisimman vähän haittaa.

Tässä tutkimuksessa käytettiin kontruktiivista tutkimustapaa. Konstruktiiviseen tutkimusotteeseen kuuluu tiivis yhteistyö liike-elämän kanssa. Tutkimuksen alussa oli tiedossa alustavasti kiinnostunut yritys, joka ei kuitenkaan lähtenyt yhteistyöhön. Tästä syystä yrityskeskeisyys jäi tästä tutkimuksessa uupumaan valitusta metodista huolimatta. Aihe ja lähestymistapa pysyivät kuitenkin käytännönläheisiä, sillä tämän tutkielman yhtenä tavoitteena oli kytkeä tieteellistä tietoa ja käytännön haasteita toisiinsa. Testattavat vaatimukset valittiin monipuolisesti. Ne sisälsivät sellaisia ominaisuuksia, jotka pystyttiin testaamaan. Osan monitori läpäisi, osaa ei. Lisäksi oli muutama vaatimus, joista ei voitu tehdä johtopäätöksiä. Ne johtuivat joko laitteen tietoliikenneyhteyksien hiljaisuudesta tai siitä, että vaatimukset tarvitsivat lisämäärityksiä. Näin erilaisia haasteita nousi esille.

9.2 Pohdinta

Turvallisuus on usein ristiriidassa muiden vaatimusten, kuten helppokäyttöisyyden, vähävirtaisuuden ja pienen koon kanssa. Turvallisuuden vaatimuksen käsittely ja tietoinen hyväksyttävän turvallisuustason määrittely voisivat auttaa turvallisuutta saamaan vipuvoimaa muita vaatimuksia vastaan. Tietoisten vähimmäisvaatimusten ja muiden määritysten pohjalta argumentointi on helpompaa kuin vain yleisen turvallisuuden peräänkuuluttamisen. Standardeista ja suosituksista voisi saada lisää taustatukea.

Kiinnostavia tutkimusaiheita on standardien soveltaminen lääkintälaitteiden elinkaaren eri osapuolten näkökulmista. Osapuolia ovat esimerkiksi ostajat, käyttäjät, testaajat ja viranomaiset sekä valmistajat. Mitkä ovat hankkijoiden ja testaajien näkemykset standardien hyödyllisyydestä ja heidän tarpeensa? Mitä viranomaiset saavat standardeista? Miten ne auttavat heitä? Miten standardit näkyvät käyttäjille? Valmistajilla on omat huolensa.

Valmistajia koskevia kysymyksiä nousee useampia. Miten erityyppiset valmistajat ottavat standardit huomioon ja kuinka vahvasti ne ohjaavat kehitystä? Ovatko turvallisuusstandardit heti uuden lääkintälaitteen ehdotuksen yhteydessä, ensimmäisen toimivan prototyypin jälkeen vai vasta viime metreillä? Miten maailmanlaajuiset toimijat sovittavat yhteen eri maiden mahdollisesti ristiriitaiset standardit? Miten nämä ristiriidat vaikuttavat liiketoimintaan? Olisiko keskitetympi standardointi kaikkien etu vai ainoastaan valmistajille edullista?

Yksi standardien haaste on niiden yleisyyden ja tarkkuuden tasapainottelu. Mitä yleisluontoisempia niiden kuvaukset ovat, sitä hitaammin ne vanhentuvat ja todennäköisesti vaativat vähemmän tarkistusta, työtä ja sovittamista muihin standardeihin. Tarkkuuden myötä standardit vanhenevat nopeammin, erityisesti tietoteknisen turvallisuuden alalla. Uusia hyökkäyksiä ilmaantuu jatkuvasti, ja käytetyt suojaustekniikat vaihtuvat toisiin. Tarkkoja kuvauksia ja testejä sisältävät standardit tulisi päivittää usein, jotta niistä olisi hyötyä eivätkä ne lukitsisi puolustusta vanhoihin toimintatapoihin. Myös tarkat standardit sitoisivat toteutusta tiettyyn malliin, joka ei välttämättä toimi kaikilla laitteilla.

Toisaalta tarkat standardit tukevat enemmän lääkintälaitteiden ostajia, valmistajia ja valvojia. Kommunikaatio helpottuu ja tuotteen oikeellisuuden toteaminen on helpompaa, jos vaatimukset ovat tarkat tai standardit sisältävät testit. Myös valmistajat voisivat olla luottavaisempia siitä, toteuttavatko heidän laitteensa kunkin standardin, kun ollaan varmoja siitä, mitä standardi tarkoittaa ja mahdollisesti testit ovat tiedossa.

Turvallisuusstandardien tarkkuudesta kaivattaneen lisää tutkimustietoa. Miten eri tarkkuusasteisiin standardeihin suhtaudutaan eri sidosryhmissä? Ovatko yleismaailmallisemmat standardit suositumpia hallinnossa ja hankinnassa yleistajuisuuden vuoksi? Vai viehättäisikö heitä enemmän tarkat standardit, jotka määrittelisivät tarkempia teknisiä vaatimuksia kaikkien puolesta ja yhteisesti, jolloin valmistajatkin todennäköisesti toteuttaisivat nämä toimenpiteet?

Miten tarkemmat tai yleismaailmallisemmat standardit vaikuttavat valmistajiin ja käyttäjiin?

Teknisempiä tutkimussuuntia olisivat käytettyjen turvatoimien toimivuus ja yleistettävyys. Mitkä menetelmät estävät pahanteon ja kuinka tarkkaan rajattuihin tilanteisiin nämä menetelmät sopivat. Mitkä menetelmät eivät sovi lääkintälaitteisiin? Esimerkiksi käytön mahdollistaminen hätätilanteissa ja niukkaresurssisuus voivat rajata autentikointimentelmiä pois. Millaisia suojauskeinoja ei voi käyttää muissa kuin lääkintälaitteissa? Viestien salausavaimen luominen sydämen sykkeen pohjalta on yksi nerokas suojauskeino, joka on tarkoitettu nimenomaan lääkintälaitteille.

Lääkintälaitteiden kyberturvallisuuteen vaikuttavat mm. määräykset ja standardit, hoidon toimivuuden vaatimus sekä rajalliset resurssit. Näidenkin kanssa navigointi on haastavaa, mutta lääkintälaitteiden kyberturvallisuus on saanut ansaitsemaansa huomiota sekä mediassa, että tiedeyhteisössä. Toivottavasti tämän huomion myötä lääkintälaitteiden kyberturvallisuuteen saadaan lisää panostusta, jotta voimme jatkossakin mennä sairaalaan turvallisin mielin.

Lähteet

Adams, Anne, ja Martina Angela Sasse. 1999. “Users Are Not the Enemy”. *Commun. ACM* (New York, NY, USA) 42, numero 12 (joulukuu): 40–46. ISSN: 0001-0782. doi:10.1145/322796.322806. http://doi.acm.org/10.1145/322796.322806.

Altawy, R., ja A. M. Youssef. 2016. “Security Tradeoffs in Cyber Physical Systems: A Case Study Survey on Implantable Medical Devices”. *IEEE Access* 4:959–979. ISSN: 2169-3536. doi:10.1109/ACCESS.2016.2521727.

Ammann, Paul, ja Jeff Offutt. 2008. *Introduction to software testing.* Cambridge University Press.

Arney, D., K. K. Venkatasubramanian, O. Sokolsky ja I. Lee. 2011. “Biomedical devices and systems security”. Teoksessa *2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society,* 2376–2379. Elokuu. doi:10.1109/IEMBS.2011.6090663.

Beckers, Kristian, Isabelle Côté, Stefan Fenz, Denis Hatebur ja Maritta Heisel. 2014. “A Structured Comparison of Security Standards”. Teoksessa *Engineering Secure Future Internet Services and Systems: Current Research,* toimittanut Maritta Heisel, Wouter Joosen, Javier Lopez ja Fabio Martinelli, 1–34. Cham: Springer International Publishing. ISBN: 978-3-319-07452-8. doi:10.1007/978-3-319-07452-8_1. http://dx.doi.org/10.1007/978-3-319-07452-8_1.

Bergenstal, Richard M., William V. Tamborlane, Andrew Ahmann, John B. Buse, George Dailey, Stephen N. Davis, Carol Joyce ym. 2010. “Effectiveness of Sensor-Augmented Insulin-Pump Therapy in Type 1 Diabetes”. PMID: 20587585, *New England Journal of Medicine* 363 (4): 311–320. doi:10.1056/NEJMoa1002853. http://dx.doi.org/10.1056/NEJMoa1002853.

Bing, Chris. 2016. “Abundance of stolen healthcare records on dark web is causing a price collapse”. *Cyberscoop* (24. elokuuta). Viitattu 25. heinäkuuta 2017. https://www.cyberscoop.com/dark-web-health-records-price-dropping/.

Bormann, C., M. Ersue ja A. Keranen. 2014. *Terminology for Constrained-Node Networks.* RFC 7228. RFC Editor, toukokuu. doi:10.17487/RFC7228. https://www.rfc-editor.org/rfc/rfc7228.txt.

Break-Glass – An Approach to Granting Emergency Access to Healthcare Systems. 2004. NEMA/COCIR/JIRA Security and Privacy Committee (SPC), joulukuu. http://www.medicalimaging.org/wp-content/uploads/2011/02/Break-Glass_-_Emergency_Access_to_Healthcare_Systems.pdf.

Burleson, W., O. Mutlu ja M. Tiwari. 2016. "Invited: Who is the major threat to tomorrow's security? You, the hardware designer". Teoksessa *2016 53nd ACM/EDAC/IEEE Design Automation Conference (DAC),* 1–5. Kesäkuu. doi:10.1145/2897937.2905022.

Burleson, Wayne, Shane S. Clark, Benjamin Ransford ja Kevin Fu. 2012. "Design Challenges for Secure Implantable Medical Devices". Teoksessa *Proceedings of the 49th Annual Design Automation Conference,* 12–17. DAC '12. New York, NY, USA: ACM. ISBN: 978-1-4503-1199-1, viitattu 7. helmikuuta 2017. doi:10.1145/2228360.2228364. http://doi.acm.org/10.1145/2228360.2228364.

Calder, Alan. 2008. *ISO27001/ISO27002 : A Pocket Guide.* IT Governance Publishing. ISBN: 9781905356706. http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=391137&site=ehost-live.

Cheremushkin, Dmitry V., ja Alexander V. Lyubimov. 2010. "An Application of Integral Engineering Technique to Information Security Standards Analysis and Refinement". Teoksessa *Proceedings of the 3rd International Conference on Security of Information and Networks,* 12–18. SIN '10. Taganrog, Rostov-on-Don, Russian Federation: ACM. ISBN: 978-1-4503-0234-0. doi:10.1145/1854099.1854106. http://doi.acm.org/10.1145/1854099.1854106.

Coatrieux, G., H. Maitre, B. Sankur, Y. Rolland ja R. Collorec. 2000. "Relevance of watermarking in medical imaging". Teoksessa *Proceedings 2000 IEEE EMBS International Conference on Information Technology Applications in Biomedicine. ITAB-ITIS 2000. Joint Meeting Third IEEE EMBS International Conference on Information Technol,* 250–255. Lokakuu. doi:10.1109/ITAB.2000.892396.

Committee on National Security Systems Instructions (CNNSI) No.4009 - National Information Assurance (IA) Glossary. 2010. Tekninen raportti. Committee on National Security Systems, 26. huhtikuuta. https://www.dni.gov/files/NCSC/documents/nittf/CNSSI-4009_National_Information_Assurance.pdf.

Common Criteria. 2017. The Common Criteria. Viitattu 21. kesäkuuta. https://www.commoncriteriaportal.org/.

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff. 2014. Tekninen raportti. Food ja Drug Administration (FDA), kesäkuu. Viitattu 5. helmikuuta 2017. http://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm356190.pdf.

CVE-2015-3955. 2015. US-CERT/NIST. https://nvd.nist.gov/vuln/detail/CVE-2015-3955.

cyber -, comb. form : Oxford English Dictionary. 2017. Viitattu 26. huhtikuuta. http://www.oed.com/view/Entry/250879?redirectedFrom=cybersecurity#eid117229282.

Cyber- Definition by Merriam-Webster. 2017. Viitattu 29. huhtikuuta. https://www.merriam-webster.com/dictionary/cyber.

Cybernetics- Definition by Merriam-Webster. 2017. Viitattu 29. huhtikuuta. https://www.merriam-webster.com/dictionary/cybernetics.

Cybersecurity | Definition by Merriam-Webster. 2017. Viitattu 26. huhtikuuta. https://www.merriam-webster.com/dictionary/cybersecurity.

Datex Ohmeda - S/5 Compact Community, Manuals, Specifications : MedWrench. 2017. MedWrench. Viitattu 27. heinäkuuta. https://www.medwrench.com/equipment/8193/datex-ohmeda-s-5-compact.

Datex-Ohmeda : Datex-Ohmeda S/5TM Central, ViewStation and Network : Technical Reference Manual. 2000. Datex-Ohmeda, syyskuu. Viitattu 28. heinäkuuta 2017.

Datex-Ohmeda : S/5TM Compact Anesthesia Monitor :S/5TM Compact Critical Care Monitor : Technical Reference Manual. 2006. Datex-Ohmeda, maaliskuu.

Definition of Cybersecurity - Gaps and overlaps in standardisation. 2016. Tekninen raportti. ENISA ja ETSI/CEN/CENELEC Cybersecurity Coordination Group CSCG, 1. heinäkuuta. doi:10.2824/4069.

Denning, Tamara, Kevin Fu ja Tadayoshi Kohno. 2008. "Absence Makes the Heart Grow Fonder: New Directions for Implantable Medical Device Security." Teoksessa *HotSec.*

Donnelly, Laura. 2017. "Largest NHS trust hit by cyber attack". *The Telegraph* (tammikuu). Viitattu 13. maaliskuuta 2017. http://www.telegraph.co.uk/news/2017/01/13/largest-nhs-trust-hit-cyber-attack/.

Neuvoston direktiivi 93/42/ETY, annettu 14 päivänä kesäkuuta 1993, lääkinnällisistä laitteista [kielellä suomi]. 1993. Tekninen raportti 169. Euroopan unionin neuvosto, 12. heinäkuuta. http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31993L0042&qid=1500376247659.

Finnegan, A., ja F. McCaffery. 2014. "A Security Argument Pattern for Medical Device Assurance Cases". Teoksessa *2014 IEEE International Symposium on Software Reliability Engineering Workshops,* 220–225. Lokakuu. doi:10.1109/ISSREW.2014.89.

Finnegan, Anita, ja Fergal McCaffery. 2015. "Towards an International Security Case Framework for Networked Medical Devices". Teoksessa *Computer Safety, Reliability, and Security: 34th International Conference, SAFECOMP 2015, Delft, The Netherlands, September 23-25, 2015, Proceedings,* toimittanut Floor Koornneef ja Coen van Gulijk, 197–209. Cham: Springer International Publishing. ISBN: 978-3-319-24255-2. doi:10.1007/978-3-319-24255-2_15. http://dx.doi.org/10.1007/978-3-319-24255-2_15.

Gayle, Damien, Alexandra Topping, Ian Sample, Sarah Marsh ja Victor Dodd. 2017. "NHS seeks to recover from global cyber-attack as security concerns resurface". *The Guardian* (13. toukokuuta). Viitattu 7. kesäkuuta 2017. https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack.

Gelperin, D., ja B. Hetzel. 1988. “The Growth of Software Testing”. *Commun. ACM* (New York, NY, USA) 31, numero 6 (kesäkuu): 687–695. ISSN: 0001-0782. doi:10.1145/62959.62965. http://doi.acm.org/10.1145/62959.62965.

Gollakota, Shyamnath, Haitham Hassanieh, Benjamin Ransford, Dina Katabi ja Kevin Fu. 2011. “They can hear your heartbeats: non-invasive security for implantable medical devices”. *ACM SIGCOMM Computer Communication Review* 41 (4): 2–13.

Greitzer, F. L., A. P. Moore, D. M. Cappelli, D. H. Andrews, L. A. Carroll ja T. D. Hull. 2008. “Combating the Insider Cyber Threat”. *IEEE Security Privacy* 6, numero 1 (tammikuu): 61–64. ISSN: 1540-7993. doi:10.1109/MSP.2008.8. http://ieeexplore.ieee.org/abstract/document/4446699/.

Halperin, D., T. S. Heydt-Benjamin, K. Fu, T. Kohno ja W. H. Maisel. 2008. “Security and Privacy for Implantable Medical Devices”. *IEEE Pervasive Computing* 7, numero 1 (tammikuu): 30–39. ISSN: 1536-1268. doi:10.1109/MPRV.2008.16.

Halperin, D., T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno ja W. H. Maisel. 2008. “Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses”. Teoksessa *2008 IEEE Symposium on Security and Privacy (sp 2008),* 129–142. Toukokuu. doi:10.1109/SP.2008.31.

Hansman, Simon, ja Ray Hunt. 2005. “A taxonomy of network and computer attacks”. *Computers & Security* 24 (1): 31–43. ISSN: 0167-4048. doi:http://dx.doi.org/10.1016/j.cose.2004.06.011. http://www.sciencedirect.com/science/article/pii/S0167404804001804.

Hu, F., D. Xie ja S. Shen. 2013. “On the Application of the Internet of Things in the Field of Medical and Health Care”. Teoksessa *2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing,* 2053–2058. Elokuu. doi:10.1109/GreenCom-iThings-CPSCom.2013.384.

Humer, Caroline, ja Jim Finkle. 2014. “Your medical record is worth more to hackers than your credit card”. *Reuters* (24. syyskuuta). Viitattu 25. heinäkuuta 2017. http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924.

IEC/TR 80001-2-2:2012: Application of risk management for IT-networks incorporating medical devices – Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls. 2012. Tekninen raportti. IEC/TR, 7. lokakuuta. https://www.iso.org/standard/57939.html.

IEC/TR 80001-2-3:2012: Application of risk management for IT-networks incorporating medical devices – Part 2-3: Guidance for wireless networks. 2012. Tekninen raportti. IEC/TR, heinäkuu. https://www.iso.org/standard/57941.html.

In Vivo | Definition by Merriam-Webster. 2017. Viitattu 29. huhtikuuta. https://www.merriam-webster.com/dictionary/in%20vitro.

In Vivo | Definition by Merriam-Webster. 2017. Viitattu 29. huhtikuuta. https://www.merriam-webster.com/dictionary/in%20vivo.

ISO/IEC 15408-1:2009: Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model. 2009. Standard. Geneva, Switzerland: ISO/IEC, 3. joulukuuta. https://www.iso.org/standard/50341.html.

ISO/IEC 15408-2:2008: Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components. 2008. Standard. Geneva, Switzerland: ISO/IEC, 19. elokuuta. https://www.iso.org/standard/46414.html.

ISO/IEC 15408-3:2008: Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components. 2008. Standard. Geneva, Switzerland: ISO/IEC, 19. elokuuta. https://www.iso.org/standard/46413.html.

ISO/IEC 27000:2016: Information technology – Security techniques – Guidelines for cybersecurity. 2016. Standard. Geneva, Switzerland: ISO/IEC, helmikuu. https://www.iso.org/standard/66435.html.

ISO/IEC 27032:2012: Information technology – Security techniques – Information security management systems – Overview and vocabulary. 2012. Standard. Geneva, Switzerland: ISO/IEC, heinäkuu. https://www.iso.org/standard/44375.html.

ISO/TC 215 Business Plan. 2013. Versio 3. ISO/TC 215 Health Informatics, 7. kesäkuuta. Viitattu 10. kesäkuuta 2017. http://isotc.iso.org/livelink/livelink/fetch/-8862396/8862414/8862423/16254633/N1245_ISOTC215_Strategic_Business_Plan_approved_posted.pdf?nodeid=16254432&vernum=-2.

ITU-TX.1205: series X: data networks, open system communications and security: telecommunication security: overview of cybersecurity. 2008. Tekninen raportti. International Telecommunication Union ITU, 18. huhtikuuta. https://www.itu.int/rec/T-REC-X.1205-200804-I.

Jalali, Samireh, ja Claes Wohlin. 2012. "Systematic Literature Studies: Database Searches vs. Backward Snowballing". Teoksessa *Proceedings of the ACM-IEEE International Symposium on Empirical Software Engineering and Measurement,* 29–38. ESEM '12. Lund, Sweden: ACM. ISBN: 978-1-4503-1056-7. doi:10.1145/2372251.2372257. http://doi.acm.org/10.1145/2372251.2372257.

Jenkins, A Milton. 1985. "Research methodologies and MIS research". *Research methods in information systems:*103–117.

Kajava, J., J. Anttila, R. Varonen, R. Savola ja J. Roning. 2006. "Information Security Standards and Global Business". Teoksessa *2006 IEEE International Conference on Industrial Technology,* 2091–2095. Joulukuu. doi:10.1109/ICIT.2006.372505.

Kansainvälinen standardointi – Suomen standardoimisliitto SFS ry. 2017. Suomen standardoimisliitto SFS ry. Viitattu 28. huhtikuuta. https://www.sfs.fi/standardien_laadinta/mita_standardisointi_on/standardisoinnin_maailmankartta/kansainvalinen_standardisointi.

Kasanen, Eero, Kari Lukka ja Arto Siitonen. 1993. “The constructive approach in management accounting research” [kielellä englanti]. Copyright - Copyright American Accounting Association Fall 1993; Last updated - 2015-08-10; SubjectsTermNotLitGenreText - US, *Journal of Management Accounting Research* 5:243. https://search.proquest.com/docview/210177084?accountid=11774.

Kaur, K., ja K. Kaur. 2016. “A study of power management techniques for Internet of Things (IoT)”. Teoksessa *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT),* 1781–1785. Maaliskuu. doi:10.1109/ICEEOT.2016.7754992.

Kerckhoffs, Auguste. 1883. “La cryptographie militaire”. *Journal des sciences militaires,* numero IX.

Kim, Y., R. Daly, J. Kim, C. Fallin, J. H. Lee, D. Lee, C. Wilkerson, K. Lai ja O. Mutlu. 2014. “Flipping bits in memory without accessing them: An experimental study of DRAM disturbance errors”. Teoksessa *2014 ACM/IEEE 41st International Symposium on Computer Architecture (ISCA),* 361–372. Kesäkuu. doi:10.1109/ISCA.2014.6853210.

Kirlappos, Iacovos, Adam Beautement ja M. Angela Sasse. 2013. ““Comply or Die” Is Dead: Long Live Security-Aware Principal Agents”. Teoksessa *Financial Cryptography and Data Security: FC 2013 Workshops, USEC and WAHC 2013, Okinawa, Japan, April 1, 2013, Revised Selected Papers,* toimittanut Andrew A. Adams, Michael Brenner ja Matthew Smith, 70–82. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-642-41320-9. doi:10.1007/978-3-642-41320-9_5. http://dx.doi.org/10.1007/978-3-642-41320-9_5.

Kitchenham, Barbara, ja Pearl Brereton. 2013. “A systematic review of systematic review process research in software engineering”. *Information and Software Technology* 55 (12): 2049–2075. ISSN: 0950-5849. doi:http://dx.doi.org/10.1016/j.infsof.2013.07.010. http://www.sciencedirect.com/science/article/pii/S0950584913001560.

Kocabas, O., T. Soyata ja M. K. Aktas. 2016. “Emerging Security Mechanisms for Medical Cyber Physical Systems”. *IEEE/ACM Transactions on Computational Biology and Bioinformatics* 13, numero 3 (toukokuu): 401–416. ISSN: 1545-5963. doi:10.1109/TCBB.2016.2520933.

Krens, Robin, Marco Spruit ja Nathalie Urbanus. 2013. “Evaluating Information Security Effectiveness with Health Professionals”. Teoksessa *Biomedical Engineering Systems and Technologies: 4th International Joint Conference, BIOSTEC 2011, Rome, Italy, January 26-29, 2011, Revised Selected Papers,* toimittanut Ana Fred, Joaquim Filipe ja Hugo Gamboa, 324–334. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-642-29752-6. doi:10.1007/978-3-642-29752-6_24. http://dx.doi.org/10.1007/978-3-642-29752-6_24.

Laki terveydenhuollon laitteista ja tarvikkeista 629/2010 [kielellä suomi]. 2017. Viitattu 13. maaliskuuta. http://www.finlex.fi/fi/laki/ajantasa/2010/20100629?search[type]=pika&search[pika]=terveydenhuollon%20laitteet.

Laszka, Aron, Mark Felegyhazi ja Levente Buttyan. 2014. “A Survey of Interdependent Information Security Games”. *ACM Comput. Surv.* (New York, NY, USA) 47, numero 2 (elokuu): 23:1–23:38. ISSN: 0360-0300. doi:10.1145/2635673. http://doi.acm.org/10.1145/2635673.

Lee, Dave. 2016. “Three US hospitals hit by ransomware” [kielellä englanti]. *BBC News* (maaliskuu). Viitattu 13. maaliskuuta 2017. http://www.bbc.com/news/technology-35880610.

Linzhang, Wang, Yuan Jiesong, Yu Xiaofeng, Hu Jun, Li Xuandong ja Zheng Guoliang. 2004. “Generating test cases from UML activity diagram based on Gray-box method”. Teoksessa *11th Asia-Pacific Software Engineering Conference,* 284–291. Lokakuu. doi:10.1109/APSEC.2004.55.

Luiijf, H. A. M., Kim Besseling, Maartje Spoelstra ja Patrick de Graaf. 2013. “Ten National Cyber Security Strategies: A Comparison”. Teoksessa *Critical Information Infrastructure Security: 6th International Workshop, CRITIS 2011, Lucerne, Switzerland, September 8-9, 2011, Revised Selected Papers,* toimittanut Sandro Bologna, Bernhard Hämmerli, Dimitris Gritzalis ja Stephen Wolthusen, 1–17. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-642-41476-3. doi:10.1007/978-3-642-41476-3_1. http://dx.doi.org/10.1007/978-3-642-41476-3_1.

Ma, Hua-Dong. 2011. “Internet of Things: Objectives and Scientific Challenges”. *Journal of Computer Science and Technology* 26, numero 6 (1. marraskuuta): 919–924. ISSN: 1860-4749. doi:10.1007/s11390-011-1189-5. https://doi.org/10.1007/s11390-011-1189-5.

Managing Information Security Risk: Organization, Mission, and Information System View. 2011. Standard. NIST, maaliskuu. doi:http://dx.doi.org/10.6028/NIST.SP.800-39.

Martin, Nigel, ja John Rice. 2011. “Cybercrime: Understanding and addressing the concersn of stakeholders”. *Computers & Security* 30 (8): 803–814. ISSN: 0167-4048. doi:https://doi.org/10.1016/j.cose.2011.07.003. http://www.sciencedirect.com/science/article/pii/S016740481100085X.

Mattern, Friedemann, ja Christian Floerkemeier. 2010. “From Active Data Management to Event-based Systems and More”. Luku From the Internet of Computers to the Internet of Things, toimittanut Kai Sachs, Ilia Petrov ja Pablo Guerrero, 242–259. Berlin, Heidelberg: Springer-Verlag. http://dl.acm.org/citation.cfm?id=1985625.1985645.

Nagamalai, Dhinaharan, Beatrice Cynthia Dhinakaran, P. Sasikala, Seoung-Hyeon Lee ja Jae-Kwang Lee. 2005. “Security Threats and Countermeasures in WLAN”. Teoksessa *Technologies for Advanced Heterogeneous Networks: First Asian Internet Engineering Conference, AINTEC 2005, Bangkok, Thailand, December 13-15, 2005. Proceedings,* toimittanut Kenjiro Cho ja Philippe Jacquet, 168–182. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-540-32292-4. doi:10.1007/11599593_13. http://dx.doi.org/10.1007/11599593_13.

Neuvonen, Pentti J. 2013. “Vakavien lääkehaittojen ja vaarallisten lääkeinteraktioiden ennakointi ja ehkäisy”. *Duodecim* 129 (1): 22–30. Viitattu 13. maaliskuuta 2017. http://www.duodecimlehti.fi/lehti/2013/1/duo10724.

NIAP. 2017. The National Information Assurance Partnership (NIAP). Viitattu 21. kesäkuuta. https://www.niap-ccevs.org/.

Pantelopoulos, A., ja N. G. Bourbakis. 2010. “A Survey on Wearable Sensor-Based Systems for Health Monitoring and Prognosis”. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* 40, numero 1 (tammikuu): 1–12. ISSN: 1094-6977. doi:10.1109/TSMCC.2009.2032660.

Peris-Lopez, Pedro, Julio Cesar Hernandez-Castro, Juan M. Estevez-Tapiador ja Arturo Ribagorda. 2009. “Cryptanalysis of a novel authentication protocol conforming to EPC-C1G2 standard”. *Computer Standards & Interfaces* 31 (2): 372–380. ISSN: 0920-5489. doi:http://dx.doi.org/10.1016/j.csi.2008.05.012. http://www.sciencedirect.com/science/article/pii/S0920548908000652.

Perry, William E. 2006. *Effective Methods for Software Testing : Includes Complete Guidelines, Checklists, and Templates.* Nide 3rd ed. Wiley. ISBN: 9780764598371. http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=158294&site=ehost-live.

Peterson, W. W., ja D. T. Brown. 1961. “Cyclic Codes for Error Detection”. *Proceedings of the IRE* 49, numero 1 (tammikuu): 228–235. ISSN: 0096-8390. doi:10.1109/JRPROC.1961.287814. http://ieeexplore.ieee.org/abstract/document/4066263/.

Piirainen, Kalle A., ja Rafael A. Gonzalez. 2013. “Seeking Constructive Synergy: Design Science and the Constructive Research Approach”. Teoksessa *Design Science at the Intersection of Physical and Virtual Design: 8th International Conference, DESRIST 2013, Helsinki, Finland, June 11-12, 2013. Proceedings,* toimittanut Jan vom Brocke, Riitta Hekkala, Sudha Ram ja Matti Rossi, 59–72. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-642-38827-9. doi:10.1007/978-3-642-38827-9_5. http://dx.doi.org/10.1007/978-3-642-38827-9_5.

Protection Profile for Security Module of General-Purpose Health Informatics Software. 2016. TURKISH STANDARDS INSTITUTION, 7. syyskuuta. https://www.commoncriteriaportal.org/files/ppfiles/HBYS_PP_07_09_2016_Updated.pdf.

Radack, S., ja R. Kuhn. 2012. "Protecting Wireless Local Area Networks". *IT Professional* 14, numero 6 (lokakuu): 59–61. ISSN: 1520-9202. doi:10.1109/MITP.2012.110.

Raitio, Riikka. 2015. "Terveyskeskusten ajanvarausongelmat ohi – turhautuneet pommittivat puheluin johtajia". *Yle* (huhtikuu). Viitattu 31. maaliskuuta 2017. http://yle.fi/uutiset/3-7903267.

Randell, B., ja J.N. Buxton, toimittaneet. 1970. *Software Engineering Techniques.* Tekninen raportti. NATO Science commitee, huhtikuu. Viitattu 7. elokuuta 2017. http://homepages.cs.ncl.ac.uk/brian.randell/NATO/nato1969.PDF.

Renaud, Karen, ja Wendy Goucher. 2014. "The Curious Incidence of Security Breaches by Knowledgeable Employees and the Pivotal Role a of Security Culture". Teoksessa *Human Aspects of Information Security, Privacy, and Trust: Second International Conference, HAS 2014, Held as Part of HCI International 2014, Heraklion, Crete, Greece, June 22-27, 2014. Proceedings,* toimittanut Theo Tryfonas ja Ioannis Askoxylakis, 361–372. Cham: Springer International Publishing. ISBN: 978-3-319-07620-1. doi:10.1007/978-3-319-07620-1_32. http://dx.doi.org/10.1007/978-3-319-07620-1_32.

Rostami, Masoud, Wayne Burleson, Farinaz Koushanfar ja Ari Juels. 2013. "Balancing Security and Utility in Medical Devices?" Teoksessa *Proceedings of the 50th Annual Design Automation Conference,* 13:1–13:6. DAC '13. New York, NY, USA: ACM. ISBN: 978-1-4503-2071-9, viitattu 7. helmikuuta 2017. doi:10.1145/2463209.2488750. http://doi.acm.org/10.1145/2463209.2488750.

Rostami, Masoud, Ari Juels ja Farinaz Koushanfar. 2013. "Heart-to-heart (H2H): Authentication for Implanted Medical Devices". Teoksessa *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security,* 1099–1112. CCS '13. New York, NY, USA: ACM. ISBN: 978-1-4503-2477-9, viitattu 7. helmikuuta 2017. doi:10.1145/2508859.2516658. http://doi.acm.org/10.1145/2508859.2516658.

Runeson, Per, ja Martin Höst. 2009. “Guidelines for conducting and reporting case study research in software engineering”. *Empirical software engineering* 14 (2): 131.

Sasse, A. 2015. “Scaring and Bullying People into Security Won’t Work”. *IEEE Security Privacy* 13, numero 3 (toukokuu): 80–83. ISSN: 1540-7993. doi:10.1109/MSP.2015.65. http://ieeexplore.ieee.org/document/7118083/.

Seaborn, Mark. 2015., 9. maaliskuuta. Viitattu 12. heinäkuuta 2017. https://googleprojectzero.blogspot.fi/2015/03/exploiting-dram-rowhammer-bug-to-gain.html.

Serrano, Jairo, Eduardo Cesar, Elisa Heymann ja Barton Miller. 2013. “Increasing Automated Vulnerability Assessment Accuracy on Cloud and Grid Middleware”. Teoksessa *Information Security Practice and Experience: 9th International Conference, ISPEC 2013, Lanzhou, China, May 12-14, 2013. Proceedings,* toimittanut Robert H. Deng ja Tao Feng, 278–294. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-642-38033-4. doi:10.1007/978-3-642-38033-4_20. https://doi.org/10.1007/978-3-642-38033-4_20.

Singh, A. K., S. G. Samaddar ja A. K. Misra. 2012. “Enhancing VPN security through security policy management”. Teoksessa *2012 1st International Conference on Recent Advances in Information Technology (RAIT),* 137–142. Maaliskuu. doi:10.1109/RAIT.2012.6194494.

Siponen, Mikko, ja Robert Willison. 2009. “Information security management standards: Problems and solutions”. *Information & Management* 46 (5): 267–270. ISSN: 0378-7206. doi:https://doi.org/10.1016/j.im.2008.12.007. http://www.sciencedirect.com/science/article/pii/S0378720609000561.

Solms, Rossouw von, ja Johan van Niekerk. 2013. “From information security to cyber security”. Cybercrime in the Digital Economy, *Computers & Security* 38:97–102. ISSN: 0167-4048. doi:dx.doi.org/10.1016/j.cose.2013.04.004. http://www.sciencedirect.com/science/article/pii/S0167404813000801.

Stigge, Martin, Henryk Plötz, Wolf Müller ja Jens-Peter Redlich. 2006. *Reversing CRC – Theory and Practice.* Tekninen raportti. Toukokuu. Viitattu 8. elokuuta 2017. http://sar.informatik.hu-berlin.de/research/publications/SAR-PR-2006-05/SAR-PR-2006-05_.pdf.

Ståhlberg, Tom. 2015. *Terveydenhuollon laitteiden lakisääteiset määräykset kansainvälisillä markkinoilla* [kielellä suomi]. Tekninen raportti. Tekes, tammikuu. Viitattu 30. tammikuuta 2017. https://www.tekes.fi/globalassets/julkaisut/terveydenhuollon_laitteiden_lakisaateiset_maaraykset_opas.pdf.

Suomen kyberturvallisuusstrategia. *Suomen kyberturvallisuusstrategia ja taustamuistio.* 2013. Turvallisuuskomitean sihteeristö. Viitattu 17. maaliskuuta 2017. http://turvallisuuskomitea.fi/index.php/fi/component/k2/14-suomen-kyberturvallisuusstrategia.

"Guide to the Software Engineering Body of Knowledge 2004 Version". 2004. *SWEBOK 2004 Guide to the Software Engineering Body of Knowledge.* Viitattu 7. elokuuta 2017. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4425813.

Taylor, Curtis R., Krishna Venkatasubramanian ja Craig A. Shue. 2014. "Understanding the Security of Interoperable Medical Devices Using Attack Graphs". Teoksessa *Proceedings of the 3rd International Conference on High Confidence Networked Systems,* 31–40. HiCoNS '14. New York, NY, USA: ACM. ISBN: 978-1-4503-2652-0, viitattu 7. helmikuuta 2017. doi:10.1145/2566468.2566482. http://doi.acm.org/10.1145/2566468.2566482.

The Art of Software Testing [kielellä English]. 2011. ID: 697721. Hoboken: John Wiley & Sons, Incorporated. ISBN: 9781118133132. http://ebookcentral.proquest.com/lib/jyvaskyla-ebooks/detail.action?docID=697721.

Tri, Jeffrey L., Jane M. Trusty ja David L. Hayes. 2004. "Potential for Personal Digital Assistant Interference With Implantable Cardiac Devices". *Mayo Clinic Proceedings* 79, numero 12 (joulukuu): 1527–1530. ISSN: 0025-6196, viitattu 14. maaliskuuta 2017. doi:10.4065/79.12.1527. http://www.sciencedirect.com/science/article/pii/S0025619611618582.

Wang, Zhi, Xuxian Jiang, Weidong Cui ja Peng Ning. 2009. “Countering Kernel Rootkits with Lightweight Hook Protection”. Teoksessa *Proceedings of the 16th ACM Conference on Computer and Communications Security,* 545–554. CCS ’09. Chicago, Illinois, USA: ACM. ISBN: 978-1-60558-894-0. doi:10.1145/1653662.1653728. http://doi.acm.org/10.1145/1653662.1653728.

Weippl, E., A. Holzinger ja A. M. Tjoa. 2006. “Security aspects of ubiquitous computing in health care” [kielellä englanti]. *e & i Elektrotechnik und Informationstechnik* 123, numero 4 (huhtikuu): 156–161. ISSN: 0932-383X, 1613-7620, viitattu 9. helmikuuta 2017. doi:10.1007/s00502-006-0336. http://link.springer.com/article/10.1007/s00502-006-0336.

Venkatasubramanian, K. K., E. Y. Vasserman, O. Sokolsky ja I. Lee. 2012. “Security and Interoperable-Medical-Device Systems, Part 1”. *IEEE Security Privacy* 10, numero 5 (syyskuu): 61–63. ISSN: 1540-7993. doi:10.1109/MSP.2012.128.

Whitman, Michael E, ja Herbert J Mattord. 2011. *Principles of information security.* Cengage Learning.

Williams, Patricia A. H. 2008. “When trust defies common security sense”. PMID: 18775827, *Health Informatics Journal* 14 (3): 211–221. doi:10.1177/1081180X08092831. eprint: http://dx.doi.org/10.1177/1081180X08092831. http://dx.doi.org/10.1177/1081180X08092831.

Wilson, K. S., ja M. A. Kiy. 2014. “Some Fundamental Cybersecurity Concepts”. *IEEE Access* 2:116–124. ISSN: 2169-3536. doi:10.1109/ACCESS.2014.2305658.

Y.2060 : Overview of the Internet of things [kielellä englanti]. 2012. Tekninen raportti. International Telecommunication Union ITU, kesäkuu. https://www.itu.int/rec/T-REC-Y.2060-201206-I.

Yao, Mariya. 2017. “Your Electronic Medical Records Could Be Worth $1000 To Hackers”. *Forbes* (14. huhtikuuta). Viitattu 26. heinäkuuta 2017. https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/.

“Defibrillaattorit yleistyvät kotona ja työpaikoilla”. 2012. *Yle* (helmikuu). Viitattu 16. elokuuta 2017. https://yle.fi/uutiset/3-5065148.

Zeadally, Sherali, Jesús Téllez Isaac ja Zubair Baig. 2016. “Security Attacks and Solutions in Electronic Health (E-health) Systems” [kielellä englanti]. *Journal of Medical Systems* 40, numero 12 (joulukuu): 263. ISSN: 0148-5598, 1573-689X, viitattu 9. helmikuuta 2017. doi:10.1007/s10916-016-0597-z. http://link.springer.com/article/10.1007/s10916-016-0597-z.

Zimmerman, T G. 1996. “Personal area networks: Near-field intrabody communication”. *IBM Systems Journal* 35 (3,4): 609–617. ISSN: 00188670. https://search.proquest.com/docview/222415082?accountid=11774.