Teemu Koskinen

Teollisen Internetin turvallisuus: Raspberry Pi kokeellisen palvelunestohyökkäyksen kohteena

Tietotekniikan pro gradu -tutkielma

6. Joulukuuta 2016

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

Pro Gradu -tutkielman tiivistelmä

Tekijä: Teemu Koskinen

Työn nimi: Teollisen Internetin turvallisuus: Raspberry Pi kokeellisen palvelunestohyökkäyksen kohteena

Koulu: Jyväskylän Yliopisto

Laitos: Tietotekniikan laitos

Päiväys: 6.12.2016

Sivuja: 47

Työn ohjaaja: Prof. Timo Hämäläinen

Teollinen Internet on yksi tämän hetken nopeiten kehittyvistä ja yleistyvistä teknologioista. Monimuotoisuutensa vuoksi sen on arveltu yleistyvän lähes kaikkeen arjen elektroniikkaan seuraavien kymmenen vuoden aikana. Turvallisuus on yksi tieto- ja viestintäteknologian suurimmista ongelmista. Uudet teknologiat tuovat mukanaan uusia turvallisuusongelmia, eikä teollinen Internet ole tässä suhteessa poikkeus.

Tässä työssä tutkittiin teollisen Internetin turvallisuusuhkia testausympäristössä käyttäen Raspberry Pi:tä, joka on yksi tehokkaimpia ja yksinkertaisimpia laitteita teollisen Internetin tuottamiseen. Jyväskylän yliopiston tietoliikennelaboratorioon pystytettiin testausympäristö, jossa kokeellinen palvelunestohyökkääjä yrittää katkaista Raspberry Pi:n välittämän suoratoistokuvan. Tutkimuksessa huomattiin Raspberry Pi:n olevan haavoittuva palvelunestohyökkäyksille, sillä sen laskentateho ei riitä puolustautumiseen moninkertaisesti tehokkaamman pöytätietokoneen hyökkäystä vastaan.

Avainsanat: Teollinen Internet, IoT, palvelunestohyökkäys, DoS, turvallisuus, Raspberry Pi

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

Abstract of the Master's Thesis

Author: Teemu Koskinen

Name of the Thesis: Security of Internet of Things: Raspberry Pi under experimental denial-of-service attack.

School: University of Jyväskylän

Department: Department of Mathematical Information Technology

Date: 6.12.2016

Number of Pages: 47

Instructor: Prof Timo Hämäläinen

Internet of Things is one of todays fastest developing and spreading technologies. Due to its versatility, it is expected to become a part of almost all everyday electronics in the coming decade. Security is one of the biggest problems in information and communications technology. New technologies bring up new security questions, and Internet of Things is no exception.

In this thesis the security threats of Internet of Things were tested in a testing environment using Raspberry Pi, which is one of the most efficient and simple devices used to produce Internet of Things. In a testing setup built in the Data Transmission Laboratory in Jyväskylä University a Denial of Service-attacker attempted to cut of a web camera stream sent by Raspberry Pi. Our study shows that Raspberry Pi is vulnerable to Denial of Service-attacks because it lacks sufficient computation capacity to defend itself against a vastly superior pc attacker.

Keywords: Internet of Things, IoT, Denial of Service, DoS, Security, Raspberry Pi

Esipuhe

Tämä työ on tehty Jyväskylän yliopiston Tietotekniikan laboratoriossa osana laitoksella tehtävää teollisen Internetin tutkimusta. Haluan kiittää työn ohjaajaa Professori Timo Hämäläistä vahvasta näkemyksestä sekä käytännön vinkeistä. Kiitän Tietotekniikan laitoksen tohtorikoulutettavaa Mikhail Zolotukhinia avusta laitteiston kanssa, sekä Erkki Häkkistä ajankohtaisen aiheen ehdottamisesta. Lopuksi haluan kiittää vanhempiani ja kihlattuani opintojeni tukemisesta.

Sisällysluettelo

Lyhenteet

ACK	Acknowledge flag – Kuittauslippu
AES	Advanced Encryption Standard – Lohkosalausmenetelmä
CSRF	Cross-Site Request Forgery
DoS	Denial of Service – Palvelunestohyökkäys
DDoS	Distributed Denial of Service – Hajautettu palvelunestohyökkäys
HDMI	High-Definition Multimedia Interface – Korkean tarkkuuden ääni- ja kuvaliitäntä
HTTP	Hypertext Transfer Protocol – Hypertekstin siirtoprotokolla
ICMP	Internet Control Message Protocol
IoT	Internet of Things – Teollinen Internet
ISP	Internet Service Provider – Internetin palveluntarjoaja
LTE	Long term evolution
LWM2M	Lightweight Machine to Machine – Kevyt käyttöinen koneiden välinen kommunoikointi
M2M	Machine to Machine – Koneiden välinen tietoliikenne
MQTT	Message Queuing Telemetry Transport
NIDS	Network Intrusion Detection System – Verkkotunkeilijan havaitsemisjärjestelmä
NFC	Near field communication
OSI	Open Systems Interconnection model
OWASP	The Open Web Application Security Project
REST	Representational state transfe
RFID	Radio-frequency identification – Radiotaajuinen etätunnistus
RTSP	Real Time Streaming Protocol – Suoratoistoprotokolla
SYN	Synchronize flag - Tahdistuslippu

TCP/IP	Transmission Control Protocol/Internet Protocol
UDP	User Datagram Protocol
WLAN	Wireless Local Area Network – Langaton lähiverkko
XSS	Cross-site Scripting

1 Johdanto

Tietotekniikan tämän hetken puhuttavimmat aiheet ovat suuri data (big data), pilvipalvelut (cloud computing) sekä teollinen Internet (Internet of things). Turvallisuus on ollut nopeasti kehittyvän tietotekniikan suurimpia kysymyksiä kautta aikain.

Tässä työssä kartoitettiin Raspberry Pi:n päälle rakennetun teollisen Internetin kamerasovellutuksen turvallisuutta. Raspberry Pi laitteena valittiin työhön sen tämänhetkisen suuren suosion perusteella. Raspberry Pi on yksi tehokkaimpia ja yksinkertaisimpia laitteita teollisen Internetin tuottamiseen. Raspberry Pi:tä on suojattu tunnetuilla ilmaisohjelmistoilla, jotka ovat pääsääntöisesti avoimeen lähdekoodiin perustuvia. Turvallisuusaukkoja lähdettiin kartoittamaan eettiseen hakkerointiin erikoistuneella Kali Linux-käyttöjärjestelmällä. Kali sisältää sisäänrakennettuna yli 600 hyökkäysohjelmaa. Eettisellä hakkeroinnilla tarkoitetaan hakkerointia, jolla etsitään laitteiden haavoittuvuuksia jatkokehittelyä ja turvallisuuden parantamista varten.

Tämä työ on tehty Jyväskylän yliopiston Tietotekniikan laboratioriossa osana laitoksella tehtävää teollisen Internetin tutkimusta. Laitteisto pystytettiin alunperin erilliseksi turvallisuustestausalustaksi. Teollisen Internetin tutkimuksen laajentuessa laitteisto saatetaan yhdistää osaksi suurempaa tutkimusalustaa.

1.1 Taustaa

Työn aiheen valintaan vaikuttivat teollisen Internetin yleistyminen sekä tämänhetkiset työtehtäväni. Työnkuvaani kuuluu teollisen Internetin pilvipalveluiden kehittäminen, ja tietoturvanäkökohdat ovat työssäni erityisen tärkeitä. Samanaikaisesti Jyväskylän yliopiston tietotekniikan laitoksella on meneillään useita teollisen Internetin prjekteja, ja IoT:n julkisten sovellutusten määrä on kasvanut yliopisto-opintojeni aikana huomattavasti. Aihe on siten erittäin ajankohtainen. Suomen valtioneuvosto julkaisi 2015 Aalto-yliopiston, Teknologian tutkimuskeskus VTT Oy:n ja Elinkeinoelämän tutkimuslaitoksen tutkimuksiin pohjautuvan raportin teollisen Internetin tarjoamista mahdollisuuksista. Raportissa teollisen Internetin povataan nostavan Suomen talouden takaisin Nokian kulta-ajan tasolle. [1] Tammikuussa 2016 Tekniikka & Talous-lehdessä puolestaan kirjoitettiin lähes 12 000 työntekijän irtosanomisesta tekniikan alalla vuonna 2015 [2]. Valtioneuvoston raportin

mukaan nykyinen talouden laskusuhdanne olisi käännettävissä kasvuksi aloittamalla rohkeasti teollisen Internetin sovellutusten kehittäminen. Teollinen Internet on tekniikan alana vielä nuori, ja arkea helpottavien innovaatioiden kehittäminen on nopeuskilpailu jossa nopein käärii isoimman potin. [1]

Esimerkkinä yksinkertaisesta arkielämää helpottavasta innovaatiosta on New Yorkin osavaltiossa White Plainsin kaupungissa kehitetty pysäköintiä auttava teollisen Internetin sovellutus. Alati kasvavassa kaupungissa oli koettu pysäköinnin olevan hankalaa. Pacen yliopisto perehtyi asiaan ja havaintojensa perusteella suunnittelivat pysäköinnin avuksi teollisen Internetin sovellutuksen. Projektissa parkkipaikoille asennettiin vapaat parkkipaikat tunnistavia antureita sekä toteutettiin mobiilisovellus, joka ilmoittaa lähellä olevista vapaista parkkipaikoista. Sovellus oli suuri menestys, koska sen pieni käyttöalue mahdollisti hyvin tarkan alueellisen tuen. A. Butowsky ym. pitivät sovellutusta tärkeänä edistysaskeleena kohti automaattiohjattua julkista- ja yksityisliikennöintiä. [3]

Teollisen Internetin kehittämisen suurimpia esteitä on tietoturva. Tietoturvan puutteellinen opetus aiheuttaa kuluttajissa tarpeettomia pelkoja ja vastustusta uuden tekniikan käyttöönotossa. Wakaza ym. käsittelevät artikkelissaan tietoturvallisuuden ymmärtämisen tärkeyttä käsiteltäessä tietoteknisiä laitteita. Heidän työnsä keskittyy Etelä-Afrikan tietoturvaopetukseen, mutta samat periaatteet ovat sovellettavissa uuden tekniikan käyttöönottoon länsimaissa. [4]

2 Teollinen Internet

Teollisesta Internetistä (Internet of things, IoT) on käytetty myös muita käännöksiä asiayhteydestä riippuen: esineiden Internet, asioiden Internet tai koneiden välinen tietoliikenne (machine to machine, M2M). Tässä työssä tulemme käyttämään termiä teollinen Internet. Käsitettä ei ole määritelty tarkasti myöskään englanniksi. Termin on ottanut käyttöön ensimmäistä kertaa Kevin Ashton vuonna 1999. Ashton kuvaili tulevaisuutta, jossa tietokoneet keräävät ja käsittelevät itsenäisesti kaiken tarvitsevansa tiedon. Tiedon avulla laitteet pystyvät ennustamaan haluttuja asioita, esimerkiksi julkisen rakennuksen etuoven kulumista. Kävijämäärää ja oven kiinni palautumista voidaan seurata anturien avulla. Jos ovi ei enää sulkeudu täydellisesti tai kävijämäärä on riittävän suuri, voidaan olettaa huoltotoimenpiteiden olevan tarpeen. Esimerkin tapaisia tietoja käytetään jo nykyään laajasti huoltotarpeen ennustamisessa, mutta tulevaisuuden teollisen Internetin on tarkoitus valvoa ja huoltaa laitteistoja täysin itsenäisesti, ilman huoltohenkilökuntaa. [5]

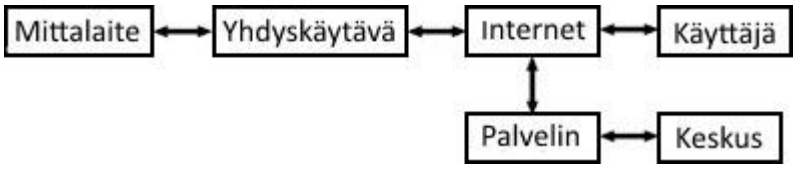
Teollisen Internetin avulla pystytään tuottamaan älylaitteita, jotka seuraavat ja valvovat omaa toimintaansa. Elektroniset laitteet ovat jo jonkin aikaa pystyneet näkemään, kuulemaan ja ajattelemaan, mutta pilvipalvelut mahdollistavat niiden välisen kommunikoinnin, ja yhdessä ne muodostavat teollisen Internetin. Tämän uskotaan johtavan mullistaviin innovaatioihin ja helpottavan suuresti jokapäiväistä elämää. [6]

Tärkeä osa laitteiden välistä kommunikointia ovat valtavasti kehittyneet langattomat tekniikat ja pilvipalvelut. Langaton Internet on nykyään lähes kaikkialla ja laitteet ovat helposti kytkettävissä siihen. Tämä mahdollistaa tiedon tallentamisen suuriin pilviarkistoihin. Teollisen Internetin laitteilla ei enää tarvitse olla itsenäistä muistia, sillä ne voivat syöttää tuloksensa suoraan pilvipalvelimille. Pilvipalvelinten suuret laskentatehot nopeuttavat tulosten analysointia.

2.1 Teollisen Internetin rakenne

Cerf ja Kristen pitävät artikkelissaan teollisen Internetin määritelmää niin väljänä, että se kattaa suuren osan modernin yhteisön teknologiasta [7]. Turvallisuustutkimuksessa käytettävän yksinkertaisen mallin rakentaminen näin laajaa määritelmää käyttäen ei ole mahdollista. Siksi valitsimme tähän työhön Alvinin ym. ehdottaman suppeamman määritelmän, jonka pohjalta rakensimme testilaitteistomme [8]. Teollinen Internet

koostuu kuudesta osiosta: mittalaite, yhdyskäytävä (gateway), Internet, palvelin (tallennus- eli pilvipalvelin), käyttäjä ja valvontakeskus (kuva 1).



Kuva 1: Teollisen Internetin rakenne [8]

Mittalaite mittaa tallennettavaa tietoa, esimerkiksi lämpötilaa. Pienin mahdollinen mittalaiteyksikkö sisältää mittapään (sensor, probe), teholähteen (power source) ja lähettimen (transmitter). Mittapää on elektroninen komponentti, jota käytetään muuttamaan fysikaalinen suure elektroniseksi signaaliksi. Tunnettuja mitattavia suureita on paljon, esimerkiksi lämpötila, kiihtyvyys ja valon aallonpituus. Tehonlähde on osa, joka välittää mittalaitteistolle sähköä. Tehonlähteenä käytetään usein akkua, mutta aurinkokenno tai suora yhteys sähköverkkoon ovat hyviä vaihtoehtoja. Lähettimen tarkoitus on lähettää mitattu tieto eteenpäin yhdyskäytävälle. Mainittavia lähetinteknologioita ovat: langaton lähiverkko (WLAN), ZigBee, Bluetooth ja Near Field Communication (NFC). Mittalaite voi olla myös hyvin monimutkainen sulautettu järjestelmä. Suuren ja monipuolisen laitteen kyseessä ollessa voidaan myös puhua mittakeskuksesta. [8]

Yhdyskäytävä on Internet-reititintä muistuttava laite, joka vastaanottaa mittalaitteen signaalin ja muuttaa sen Internet-yhteensopivaan muotoon. Suuremmat mittalaitteet voivat myös itse hoitaa pääsyn Internettiin, jolloin yhdyskäytävä on hoidettu ohjelmallisesti.

Internet on maailmanlaajuinen tietokoneiden verkosto. Klassisesti Internet muodostuu palvelimista ja niiden yhteydestä toisiinsa. Palvelin on tietokone, joka sisältää tietoa, ohjelmia tai palveluita käyttäjille. Internetin käyttäjä kytkeytyy verkkoon omalla tietokoneella palveluntarjoajan (Internet service provider, ISP) avulla. Klassinen Internet perustuu TCP/IP-protokollaan (transmission control protocol/Internet protocol), jossa kaikki liikenne tapahtuu pakettien avulla. Tulevaisuuden Internet (future Internet) on tehnyt tuloaan 2000-luvun alkupuolelta asti. Käsitteellä viittataan uusiin arkkitehtuureihin sekä tapoihin, joilla tietoa voidaan välittää tehokkaammin ja liittää uutta tekniikkaa olemassa olevaan verkkoon. Näitä uusia tekniikoita ovat esimerkiksi

iso data, pilvipalvelut sekä tämän tutkimuksen aiheena oleva teollinen Internet. [9]

Tallennus- eli pilvipalvelin on tietovarasto, jonne arkistoidaan kaikki mittalaitteiden lähettämä tieto, jolloin se on valvontakeskuksen ja tarkoituksenmukaisten käyttäjien saatavilla. Valvontakeskus valvoo ja ohjaa koko järjestelmää ja voi tehdä tarvittaessa korjaustoimenpiteitä saadun datan perusteella. Tarkoituksenmukaiset käyttäjät voivat käyttää pilvipalvelimelle tallennettua mittaustietoa haluamaansa tarkoitukseen. Esimerkiksi sademäärän mittaaminen mahdollistaa tulevan sadon ennustamista.

Al-Fuqaha ym. ovat ehdottaneet artikkelissaan teoreettisempaa mallia teollisesta Internetistä. He ovat jakaneet teollisen Internetin kolmeen kerrokseen: havaintokerrokseen (perception layer), verkkokerrokseen (network layer) ja sovelluskerrokseen (application layer), jolla on erikseen ala- ja ylätaso. Al-Fuqaha ym. huomauttavat, että tämä abstrakti kerrosteoria ei vastaa todellista teollista Internetiä, eikä se pysty kattamaan edes kaikkia tämän hetken teknologioita. Silti he ovat vahvasti sitä mieltä, että se on yksinkertaisista malleista kattavin. [6]

Al-Fugahan ym. esittämässä mallissa havaintokerrokseen kuuluvat kaikki fyysiset mittalaitteet. Kerroksen tarkoitus on muuntaa ympäröivästä maailmasta tehdyt mittaukset digitaaliseen muotoon ja lähettää tiedot turvallista kanavaa pitkin verkkokerrokseen.

Verkkokerroksessa on Al-Fuqahan ym. mukaan kolme alakerrosta: laiteabstraktio (object abstraction), palvelujen hallinta (service management) ja sovelluskerros (application layer). Abstraktiokerroksessa tapahtuu mitatun tiedon siirto palvelujen hallintaan. Kyseisen kerros sisältää kaikki tiedonsiirtoteknologiat sekä tiedon muokkauksen ja hallinnan. Tällä tarkoitetaan sitä, että mittalaite siirtää tietonsa yhdyskäytävälle ja yhdyskäytävältä Internetin kautta palvelimelle laskentaa varten. Palvelujen hallinta on verkkokerroksen päättävä elin. Kun tieto on päätynyt palvelimelle on palvelujen hallinnan mahdollista suorittaa tiedolla laskelmia, joiden avulla hallinta tekee päätöksiä sekä lähettää käskyjä tehtyjen päätösten mukaan.

Verkkokerroksen alatason sovelluskerros on sen käyttäjille näkyvä osa. Sovelluskerroksen kautta käyttäjä voi tehdä erinäisiä palvelupyyntöjä, esimerkiksi pyytää paikallisia säätietoja. Ylätason sovelluskerrosta nimitetään myös liiketoimintakerrokseksi. Tämän kerroksen tarkoitus on hallinnoida ja seurata koko teollisen Internetin palveluja. Liiketoimintakerroksessa toimivat kaikki ylemmän tason

ohjelmistot, jotka mahdollistavat mitattujen tietojen perusteella määrittämistä, kehitystä, seurantaa, analysointia, suunnittelua ja päätöksentekoa. Ilman tätä kerrosta teollinen Internet ei toimi automaattisesti ja on käytännössä vain laaja mittausjärjestelmä.

2.2 Teollisen Internetin toiminnallisuuksia

Al-Fuqaha ym. ovat tunnistaneet kuusi tärkeää osa-aluetta, jotka saavat teollisen Internetin toimimaan sekä auttavat ymmärtämään tätä laajaa käsitettä. Nämä ovat tunnistaminen, havainnointi, viestintä, laskenta, palvelut ja semantiikka. Tunnistaminen (identification) viittaa laitteiden tunnistamiseen verkossa. Kaikkien laitteiden tulisi olla yksilöitävissä. Laitteilla on oma tunnus sekä sisäisen verkon IP osoite. Nimeämisessä tulisi käyttää riittävän tunnistettavia nimiä, jotta laitteet voidaan tunnistaa suuremmassakin verkostossa. Useilla laitteilla on todennäköisesti sama IP-osoite eri lähiverkoissa, joten laitteen tunnuksen olisi hyvä sisältää myös tieto siitä, missä verkossa se on.

Havainnointi (sensing) on toiminnallisuus, jossa kerätään tietoa ympäröivästä maailmasta ja lähetetään palvelimelle säilöön tai käsiteltäväksi. Yleisiä mittauskohteita ovat fysikaaliset suureet sekä esimerkiksi erilaisten tapahtumien lukumäärät.

Viestinnän (communication) tarkoitus on yhdistää laitteet langattomasti ja sujuvasti toisiinsa. Teollinen Internet käyttää pääasiassa langattomia verkkoja (WiFi), koska niiden määrä on lisääntynyt suuresti, mutta käyttökohteesta riippuen käytössä on laaja kirjo erilaisia langattomia viestintäteknologioita. Esimerkiksi Z-wave on jossain määrin suosittua automaation parissa. Kyseessä on suurelle yleisölle ehkä hieman tuntemattomampi teknologia, jonka etuna on WiFiin nähden pienempi virrankulutus. Lyhyen kantaman langattomat teknologiat RFID ja NFC ovat puolestaan käytössä fyysisten tuotteiden merkitsemisessä automaattisessa tunnistamisessa. LTE (long term evolution), joka tunnetaan paremmin 4G:nä, on tärkeä langaton teknologia liikkuvissa kohteissa kuten autoissa ja junissa. Viestintäteknologia, kuten kaikki muutkin teknologiavalinnat, riippuu suuresti teollisen Internetin arkkitehtuurista. Pienten mittapäiden ja laitteiden vähäinen teho ja energiakapasiteetti rajoittavat niille saatavilla olevia teknologiaratkaisuja.

Laskenta (computation) jaetaan laitteistoon ja ohjelmistoon, jotka muodostavat yhdessä tehokkaan laskenta-alustan. Taulukossa T1 on lueteltu muutamia tunnetuimpia laitteistoja tässä työssä käsitellyn Raspberry Pi:n ohella. Mittalaitteistot suunnitellaan

usein mahdollisimman pieniksi ja yksinkertaisiksi. Esimerkiksi lämmön mittaamiseen ja tiedon välitykseen riittää yksinkertainen mikrokontrolleri, anturi sekä WiFi-sovitin. Laitteissa käytettävät ohjelmistot valitaan tilanteen mukaan. Myös ohjelmistojen suunnittelussa ja asennuksessa pyritään yleensä siihen, että ne olisivat mahdollisimman kevyitä eivätkä sisältäisi mitään tarpeetonta. Pilvipalvelut ovat teollisen Internetin toinen suuri laskentaosio mittalaitteistojen ohella. Niiden laitteet ja ohjelmistot ovat usein massiivisia, sillä niiltä vaaditaan suuria määriä muistia ja laskentatehoa.

Palvelut (services) jaetaan Al-Fugahan ym. mukaan neljään luokkaan: identiteetti pohjaisiin palveluihin (identity-related), tiedon keruu palveluihin (information aggregation services), yhteisen tietoisuuden palveluihin (collaborative-aware services) ja kaikkialla läsnä oleviin palveluihin (ubiquitous services). Identiteettiin liittyvillä palveluilla tarkoitetaan laitteiden tunnistamista, ja kyseistä palvelua käytetään aina kun laitetta seurataan tai käsketään. Tiedonkeruupalvelut kokoavat yhteen teollisen Internetin ohjelmistojen käyttöön kerättävän tiedon. Yhteinen tietoisuus tutkii kerättyä tietoa ja reagoi sen mukaisesti. Kaikkialla läsnäoleva palvelu on teollisen internetin tavoitteena oleva ihanteellinen palvelumuoto, joka määrittelee itsenäisesti parhaan mahdollisen toimintatavan missä tahansa tilanteessa. Toistaiseksi tällaista palvelua ei ole vielä olemassa.

Teollisen Internetin kuudes osa-alue Al-Fugahan ym. mukaan on semantiikka, jolla viitataan teollisen Internetin älykkääseen tiedonkeruuseen ja kykyyn tarjota palveluja keräämänsä tiedon perusteella. Tiedonkeruu tarkoittaa tiedon havaitsemista, keräämistä ja niiden avulla mallintamista, joiden perusteella palveluja tarjotaan. Al-Fugahan ym. mukaan semantiikka on teollisen Internetin aivot. [6]

2.3 Kehittämiskohteita

Markkinoiden kehitys viittaa siihen, että teollisen Internetin kehittämisestä on hyötyä monilla aloilla, ja siihen ollaan suuresti panostamassa lähitulevaisuudessa. Esimerkiksi mobiililaitteiden käyttö sairauksien ennaltaehkäisyssä, seurannassa ja hoidossa tarjoaa uusia ratkaisuja terveydenhuollon käyttöön. Perinteisten laitteiden kehittäminen älylaitteiksi on myös muodissa. Saavuttaakseen täyden potentiaalin teollisen Internetin pitää kuitenkin vielä kehittyä ideatasolla ja konkretisoitua erinäisten sopimusten muodossa. Sopimuksilla pyritään varmistamaan, että laitteet ja ratkaisut ovat yhteensopivia ja toimivat mahdollisimman laajasti kaikkialla maailmassa, yhteisiä

standardeja ja käytäntöjä noudattaen. Protokollia tarvitaan erilaisten laitetyyppien yhdistämiseen. Esimerkiksi älyauton tulisi olla yhteensopiva kaikenlaisten markkinoilla olevien kännykkätyyppien kanssa, merkistä riippumatta. Tavoitteena on, että eri valmistajien laitteet toimisivat harmonisesti yhdessä. Internet arkkitehtuuria pitää myös kehittää suurien laitemäärien takia. Evansin mukaan Internet-laitteiden lukumäärä ylitti ihmisten väkiluvun vuonna 2010, jolloin maailmassa oli 1.84 Internet-laitetta henkilöä kohti [10]. Määrän uskotaan myös kasvavan sitä mukaa kun teollinen Internet kehittyy. Internetprotokolla versio 6 (Internet protocol versio 6, Ipv6) ratkaisi aikanaan laitemäärien aiheuttaman ongelman, mutta ratkaisu ei ole välttämättä riittävä teollisen Internetin yleistyessä. [6]

Al-Fugaha ym. ovat jakaneet tulevaisuuden teollisen Internetin kehityskohteet kahdeksaan osa-alueeseen: saatavuus (availability), luotettavuus (reliability), liikkuvuus (mobility), suorituskyky (performance), hallinta (management), skaalautuvuus (scalability), käyttöominaisuuksien päällekkäisyydet (interoperability) ja turvallisuus ja yksityisyys (security and privacy). Teollisen Internetin saatavuus pitää huomioida laitteisto- ja ohjelmistotasolla, jotta saadaan aikaiseksi kaikkialla ja kaiken aikaa toimivia palveluja. Ohjelmistotasolla tämä merkitsee sitä, että useita käyttäjiä on mahdollista palvella samanaikaisesti. Laitteistotasolla tämä merkitsee ympärivuorokautista toimivuutta sekä yhteensopivuutta ohjelmistojen kanssa.

Luotettavuudella tarkoitetaan järjestelmän kykyä toimia toivotulla tavalla. Uusien laitteiden tai ohjelmistojen lisääminen on mahdollista vain silloin, kun aiempi järjestelmä toimii määritelmien mukaan. Mikäli määritelmiä ei noudateta, syntyy palveluun virheitä ja mahdollisia katkoksia. Mahdollisten häiriöiden ja katkosten on myös oltava nopeasti korjattavissa, ja niiden aikana olisi suositeltavaa olla olemassa korvaavia ratkaisuja, jotka estäisivät palvelun katkeamisen käyttäjiltä ja tietojen menetyksen. Luotettavuus on pidettävä mielessä niin ohjelmisto- kuin laitteistosuunnittelussa.

Liikkuvuus tuottaa monenlaisia ongelmia teollisen Internetin sovellutuksille. Mobiilikäyttäjä vaihtaa verkkoa satunnaiseti, liikkuu verkkojen välimaastossa tai jopa verkkojen ulkopuolella. Myös aiemmin mainittu käyttäjämäärien nopea kasvu aiheuttaa mobiiliratkaisujen hallinnoinnille ongelmia. Verkkojen tulisi olla kattavia ja ennakoida myös käyttäjän joutuminen hetkellisesti verkon ulkopuolelle. Myös suorituskyky tulee olemaan tärkeä kehityskohde teollisen Internetin kasvaessa. Kun verkkoon on yhdistetty

samanaikaisesti suuri määrä erilaisia laitteita, teollisen Internetin suorituskyky joutuu kovalle koetukselle. Toisaalta suorituskykyä voidaan helposti testata jo kehitysvaiheessa erilaisilla kuormitustesteillä.

Suurien laite- ja ohjelmistomäärien hallinta ja skaalautuvuus eli tilanteen mukainen sopeutuminen on haastavaa. Tähän tarkoitukseen on kehitteillä standardeja, jotta hallintaan käytettävät tekniikat olisivat mahdollisimman samanlaisia ja yhteensopivia. Al-Fugaha ym. pitivät artikkelissaan kevytkäyttöisen koneiden välisen kommunikointiprotokollan (lightweight machine to machine, LWM2M) kehitystä tärkeänä kehitysaskeleena kohti standardisoitua teollista Internetiä. Protokollan on tarkoitus helpottaa laitteen ja palvelimen välistä kommunikaatiota, hallita resursseja sekä tietopaketteja. Skaalautuvuudella tarkoitetaan ohjelmiston kykyä toimia samalla nopeudella laitemäärien ja toimntojen kasvusta huolimatta. Tähän pyritään hajauttamalla ja ohjaamalla toimintoja vähemmän kuormitetuille yksiköille.

Käyttöominaisuuksien päällekkäisyyksillä viitataan edellä mainittuun laitekannan monimuotoisuuteen ja yhteensopivuuden haasteisiin. Esimerkiksi kännykkä saattaa käyttää useita langattomia tiedonvälitysmenetelmiä, jotka eivät saisi estää toistensa toimintaa. Turvallisuus- ja yksityisyysongelmista tärkein Al-Fugahan ym. mukaan on tunnistautumisavainten jakaminen keskenään erilaisten laitteiden välillä. Teollisen Internetin tietopaketit kulkevat miljoonien pienten laiteyhteyksien läpi, ja jokainen kohta on alttiina hyökkäykselle. Kaikki kehityskohteet ja ongelmat Al-Fugahan ym. artikkelissa liittyvät laitteiden ja ohjelmistojen valtavan monimuotoiseen joukkoon ja niiden yhteensovittamisen haasteellisuuteen. Teollisen Internetin laajuus on sen suurin hyöty ja samalla ongelma. [6]

2.4 Teollisen Internetin yleiset standardit

Useat lähteet ovat yrittäneet kuvailla teollisen Internetin rakennetta luomalla siitä erilaisia malleja ja yksinkertaistuksia. Al-Fugaha ym. ovat koonneet kehittämälleen teollisen Internetin mallille myös tärkeitä protokollia ja standardeja. [6] Eri tasojen teknologioiden tunteminen ei ole tämän työn kannalta oleellista. On tärkeää kuitenkin ymmärtää, että eri osa-alueiden standardit ovat hyvin vaihtelevia ja teknologiariippuvaisia. Niiden keskinäinen kommunikointi ja kommunikointi toisen tason kanssa on heikosti standardisoitu. Yksittäisten laite- ja ohjelmistovalmistajien tekemät erilaiset ratkaisut tuottavat pidemmän päälle ongelmia suurien kokonaisuuksien

luonnissa, josta teollisessa Internetissä on pääsääntöisesti kyse. [6] Seuraavissa aliluvuissa (2.4.1 - 2.4.4) esitellään teollisen Internetin tuottamiseen käytettyjä standardisoituja tekniikoita. Näiden avulla on mahdollista luoda yhdenlainen teollisen Internetin kokonaisuus.

2.4.1 MQTT-viestinvälitysprotokolla

MQTT on lyhenne sanoista Message Queuing Telemetry Transport. MQTT-viestinvälitysprotokolla on tarkoitettu lyhyeen ja yksinkertaiseen viestittämiseen. Tämä mahdollistaa viestien välittämisen hankalasti tavoitettaviin kohteisiin ympäristöissä, joissa esiintyy suuria viiveitä tai alhaisia kaistanleveyksiä. MQTT toimii TCP/IP-protokollan päällä, joten se on helposti yhteensovitettavissa muun verkkoliikenteen kanssa.

MQTT-protokollassa on kolme tärkeää toimijaa: julkaisija (publisher), välittäjä (broker) sekä tilaaja (subscriber). Julkaisija on teollisen Internetin tapauksissa usein mittalaite, joka lähettää mitattuja tuloksia kohti pilveä. Välittäjä on usein ohjelmisto, joka jakaa julkaisijan lähettämiä tietoja valitulla aiheella (topic). Tilaaja on joko pilvi tai suoraan käyttäjä, joka tilaa tietyn aiheen sanomat itselleen. MQTT-protokolla tukee myös viestien vastaanottamisen vahvistusta, jotta tärkeiden viestien perille saaminen on taattua. [11, 12]

2.4.2 REST-arkkitehtuuri

REST-arkkitehtuuri, lyhenne sanoista Representational state transfer, on rakennemalli, joka sopii teollisen Internetin tuottamiseen. REST on HTTP-protokollan päällä toimiva suurille yhteysmäärille toimiva rakennemalli. REST muodostuu neljästä yksinkertaisesta operaatiosta: hae (get), aseta (put), tee (post), poista (delete). ”Hae” on kyselyoperaatio, jolla pyydetään palvelinta lähettämään tietoa. ”Aseta” on pyyntöoperaatio, jota usein käytetään tallentamaan tai muuntamaan tietokannan tietoja. ”Tee” on yleiskäyttöinen pyyntöoperaatio, jota voidaan käyttää kerätyn tiedon ulkopuolisiin toimintoihin esim. näytettävän tiedon rajaamiseen tai käyttäjän ulos- ja sisäänkirjaamiseen. ”Poista” on suoraviivainen käskyoperaatio, jota käytetään poistamaan tietoja tietokannasta. Näiden neljän operaation avulla luodaan yhdenmukainen rajapinta, jota voidaan käyttää useiden ohjelmistojen ja laitteiden toimesta. Esimerkiksi nettisivut ja kännykkäapplikaatio käyttävät samaa

kyselykomentoa saadakseen mittalaitteen lähettämät tulokset tietokannasta näyttöpäätteelle. [13, 14]

2.4.3 AES-salaus

AES-salaus, Anvanced Encryption Standard, tunnetaan myös nimellä lohkosalausmentelmä. AES-salauksen tekniikka on yleisesti tunnettu, ja sen turvallisuutta on siksi myös kritisoitu [15]. Salattava lukukelpoinen teksti yhdistetään salausavaimeen usealla monimutkaisella aritmeettisella laskutoimituksella. Aritmeettiset laskutoimitukset on tarkkaan määritetty AES-salaustekniikassa, koska niitä tarvitaan salauksen purkuun. Salauksen toiminta perustuu lähettäjän ja vastaanottajan välille jaettuun salausavaimeen. AES-salausta pidetään riittävänä salauksena, mikäli salausavain ei vuoda. AES-salauksen suurimpia heikkouksia on avainten ennalta asentaminen tuotannossa tai Internetin yli uusiminen. Teollisen Internetin näkökulmasta on tärkeää, että AES-salaus voidaan toteuttaa laitteistotasolla tai ohjelmistotasolla. [15, 16]

2.4.4 OSI-malli ja OSI-johdanteinen IoT-A-malli

OSI-malli, Open Systems Interconnection model, on seitsenkerroksinen tiedonsiirtoon keskittyvä standardisoitu rakenne. OSI-mallissa tiedonsiirtokerrokset ovat: fyysinen kerros, siirtokerros, verkkokerros, kuljetuskerros, istuntokerros, esitystapakerros ja sovelluskerros.

Fyysinen kerros määrittelee tiedonsiirtoverkon fyysisen rakenteen eli topologian. Teollinen Internet on usein tähtitopologian mallinen, jossa kaikki tiedonsiirto tapahtuu keskipisteen, pilven, kautta. Siirtokerros määrittelee fyysisten laitteiden yhteyden. Kerros myös tarkkaillee mahdollisia virheitä, joita saattaa tapahtua siirryttäessä fyysiseltä laitteelta verkkoon. Verkkokerros hallinnoi laitteiden osoitekarttaa ja mahdollistaa tiedon kulun verkosta toiseen. Osoitekartan avulla verkkokerros määrää yhdistettäviä laitteita. Kuljetuskerros seuraa datapakettien kulkemista. Tarkka seuranta mahdollistaa luotettavan tiedonkulun ja ilmoitukset mahdollisista virhetilanteista. Istuntokerros pitää huolen siitä, että yhteydessä olevat laitteet ovat samassa tilassa. Mikäli teollisen Internetin ratkaisua ohjataan useasta osoitteesta, on tärkeää, että kaikki näkymät päivittyvät samanaikaisesti. Esitystapakerros huolehtii salauksesta ja sen purkamisesta. Kerros esimerkiksi purkaa lähetetyn tiedon salauksen ja toimittaa

sovelluskerrokselle tiedon selkokielisenä. Sovelluskerros mahdollistaa sovellusten kiinnittymisen systeemiin.

Alhamedi ym. soveltavat työssään OSI-mallia teollisen Internetin rakenteeseen muodostaen IoT-A -mallin. IoT-A:n etuina on yksi selkeä turvallisuuskerros ja yksi tiedonvälityksen tarkkailija, ja niiden toiminta on myös helpommin toteutettavissa pienille ja tehottomille teollisen Internetin laitteille. IoT-A-malli muodostuu fyysisestä näkökulmasta, yhteysnäkökulmasta, IP/ID -näkökulmasta, Päästä päähän -näkökulmasta sekä tietonäkökulmasta. Fyysinen näkökulma on yksi yhteen OSI-mallin fyysisen kerroksen kanssa. Yhteysnäkökulma koostuu räätälöidyistä yhteysjärjestelmistä ja turvallisuusratkaisuista. Tämän näkökulman on tarkoitus pystyä yhdistämään teollisen Internetin heterogeeninen laitekanta. IP/ID -näkökulma on OSI-mallin verkkokerros ja siihen lisättynä tunnistetietoja, joiden avulla voidaan paremmin erotella teollisen Internetin tuotteet toisistaan. Päästä päähän -näkökulma korostaa luotettavaa tiedonvälitystä koko systeemin lävitse. Useiden verkkoympäristöjen lävitse pääseminen vaatii tarkoja rajapintamääritelmiä ja läpinäkyvyyttä. Tietonäkökulma on järjestelmän päällimmäinen tarkoitus. Teollisen Internetin ratkaisun on tarkoitus kuljettaa luotettavasti tietoa langattomasti laitteelta toiselle. [17]

3 Tietoturva

Tietoturva on hyvin laaja käsite, jota käsitellään tässä kolmesta näkökulmasta: turvallisuus (security), yksityisyys (privacy) ja luottamus (trust). Turvallisuudella tarkoitetaan puolustautumista ulkopuolisilta hyökkäyksiltä. Turvallisuutta mallinnetaan toiminta- ja hyökkäysmallien avulla. Luottamuksella viitataan teollisessa Internetissä oikeellisuuteen. Useat mittalaitteet saattavat mitata samaa asiaa, mutta jos niiden mittaustulokset ovat keskenään ristiriidassa, mistä voidaan tietää mikä mittaustulos on oikea? Virheellinen tieto saattaa johtaa vääriin johtopäätöksiin, jolloin seurauksena voi olla vaaratilanteita tai rahallisia tappioita. Yksityisyys viittaa tiedon säilymiseen oikeilla henkilöillä tai laitteilla. Palvelin yhdistelee sille tallennettua tietoa olemassa olevan tiedon kanssa ja tekee siitä päätelmiä, jolloin on tärkeää varmistua siitä, että käyttäjä pääsee käsiksi vain niihin tietoihin, joihin hänellä on oikeus.

Tietoturvan kääntöpuolena on usein käytettävyys tai toimivuus. Liiallinen tiedon yksityisyys tai turvallisuus estää monimutkaisiempien laskentamallien käytön tietojen käsittelyssä. Rajallinen tieto estää kokonaiskuvan hahmottamista, jolloin johtopäätökset jäävät vajaiksi ja saattavat vääristyä pahasti. Hyvä esimerkki tietoturvan ja toimivuuden ristiriidasta on savun tunnistava videokamera. Savuntunnistus on tehokas turvallisuutta lisäävä ratkaisu, mutta kuvattavan kohteen yksityisyydensuoja saattaa rajoittaa sovelluksen laajempaa käyttöä esimerkiksi kotitalouksissa. [18]

3.1 Teollisen Internetin tietoturvasta yleisesti

Rolf H. Weberin mukaan teollisen Internetin tietoturvalla on neljä osa-aluetta: hyökkäyksenkestokyky (resilience to attacks), tiedon todentaminen (data authentication), kulunvalvonta (access control) ja asiakkaan yksityisyys (client privacy) [19].

Teollisen Internetin hyökkäyksensietokyvyn pitäisi olla niin hyvä, että järjestelmä pystyy välttämään tunnetut hyökkäystyypit ja mahdollisten ilmoitusten perusteella korjaamaan pieniä tietovuotoja. Tiedon todentamisella tarkoitetaan halutun tiedon ja pyytäjän osoitteen aidoksi todistamista. Kulunvalvonta on määritelty siten, että hankittuihin tietoihin pitää olla hallittu pääsy. Yksityisyyden säilymistä voidaan pitää käyttäjän ihmisoikeutena. Vuonna 2009 Euroopan komissio on antanut radiotaajuisen etätunnistuksen (radio-frequency identification, RFID) ja teollisen Internetin

yksityisyyden suojaamisesta suosituksen, jonka mukaan sovellusten tulee olla lainmukaisia, eettisiä sekä sosiaalisesti ja poliittisesti hyväksyttäviä. Tekniikan ja turvallisuusratkaisujen kehittämistä hidastaa se, että siinä on välttämätöntä huomioida paikallinen lainsäädäntö sekä eettiset näkökulmat. [19]

3.2 Teollisen Internetin eri osien tietoturvallisuus

Teollisen Internetin määritteleminen ja mallintaminen on vaikeaa, kuten edellä on kuvattu, joten myös sen turvallisuuden määrittäminen on vaikeaa. Käytämme tässä kappaleessa 2.1 esitettyä teollisen Internetin määritelmää, jotta aiheeseen saadaan selkeä rajaus. Määrittelimme teollisen Internetin koostuvan kuudesta osasta: mittalaite, yhdyskäytävä, Internet, palvelin, käyttäjä ja valvontakeskus. Seuraavaksi käsittelemme kunkin osan turvallisuutta erikseen.

Mittalaite itsessään on hyvin vaihteleva kokonaisuus. Mitattavia asioita on paljon ja kaikilla niillä on omat mittaustekniset ongelmat. Esimerkiksi lämpömittarin luotettavuuteen vaikuttaa sen sijainti. Laitteen mittaaman lukeman pitäisi edustaa hyvin alueella vallitsevaa lämpötilaa. Mikäli laite on suorassa auringonpaisteessa, saattaa mitattu lämpötila olla useita asteita liian korkea. Sädemäärän tai valonmäärän mittauksisa erinäiset rakenteet saattavat vaikeuttaa mitattavan suureen pääsyä mittarille. Esimerkeissä on kysymys laitteen fyysisestä tietoturvasta. Mittalaitteen fyysinen turvallisuuskin voi vaarantua, mikäli ulkopuoliset henkilöt pääsevät käsiksi laitteeseen. Vandalismi voi tulevaisuudessa tuottaa suuriakin ongelmia sekä rahallisia menetyksiä kalliiden IoT-laitteiden asennuksissa julkissa tiloissa. [20] Ulkopuolisten pääsy mittalaitteelle on myös tietoturvariski. Pahimmassa tapauksessa mittalaite on uudelleenohjelmoitavissa ja sen haltuunotto on mahdollista. Huomaamattomampia tapoja on pyytää laitetta lähettämään tiedot myös hyökkääjälle, mikäli mitattu tieto on arvokasta. Useimmat teollisen Internetin mittalaitteet ovat myös alttiita ylivoimalle (overpower), sillä ne ovat tavallisesti pieniä ja vähän energiaa kuluttavia laitteita. Esimerkkejä ylivoimahyökkäyksistä ovat tulvahyökkäykset ja ehtymishyökkäykset, joissa hyökkääjä kuluttaa laitteen energian ja tekee sen toimintakyvyttömäksi. [21]

Mittalaitteen fyysisestä suojauksesta huolehditaan yleensä hyvällä koteloinnilla, huomaamattomalla sijoittelulla tai lukitulla sijainnilla. Ylimääräiset sisään- ja ulostulot on syytä peittää tai tukkia, jottei niihin ole mahdollista kytkeytyä. Mittalaitteen toiminta on usein suojattu salausavaimilla. Salausavain tarvitaan, että mittalaitetta voidaan

uudelleenohjelmoida tai lukea mittalaitteen lähettämää dataa. Salaustekniikka eli kryptologia on tieteenala, jossa tutkitaan turvallista viestintää. Salaustekniikka on yksi tärkeimmistä teollisen Internetin toiminnan turvaajista. [20]

Yhdyskäytävän tarkoitus on yhdistää mittalaite Internetiin. Internetin myötä mittalaitteeseen kohdistuvat yleisesti tunnetut uhat: virukset ja luvattomat käyttäjät. Riippuen halutusta arkkitehtuurista on virustorjunta ja palomuuri mahdollista sijoittaa joko mittalaitteeseen tai yhdyskäytävään. Ideaalisessa tapauksessa tämän pitäisi riittää, mutta on muistettava, että kyseisissä ohjelmistoissakin on tietoturva-aukkoja. [21]

Yhdyskäytävän jälkeen salattu tieto päätyy Internetiin. Tiedon suojana on tässä vaiheessa ainoastaan tehty salaus. Kuka tahansa salausavaimen omaava henkilö voi lukea paketin tiedot. Usein käytetään valmiita ratkaisuja ja luotetaan niiden turvallisuuteen. Yritysten teettämissä riskianalyyseissä lasketaan, kuinka suuria menetyksiä tietovuodot saattavat aiheuttaa, sekä harkitaan turvallisuuden lisäämisen tarvetta. Salausavaimella salattu tieto kulkee Internetin yli palvelimelle, jolla tieto saatetaan purkaa ja salata eri avaimella tai säilyttää alkuperäisessä salauksessa tiedonhaun nopeuttamiseksi. Palvelin on usein suojattu mittalaitteen tavoin palomuurilla ja virustorjunnalla. [21]

Valvontakeskus tai käyttäjä saavat tiedot palvelimelta omilla tunnuksillaan. Tunnuksilla saatavat tiedot on usein rajattu käyttäjäkohtaisesti. Käyttäjällä saattaa olla esimerkiksi pääsy senhetkiseen sadetilanteeseen, kun taas valvontakeskuksessa voidaan tarkastella koko kuukauden sademääriä. Useissa tutkimuksissa on havaittu suurimpien tietoturvariskien olevan käyttäjien aiheuttamia. Syynä on tavallisesti tiedon ja osaamisen puute tai välinpitämättömyys sekä inhimilliset virheet.

3.3 Tietoturvallisen teollisen Internetin tuottamisen haasteet

Tuenin mukaan teollista Internettiä rajoittaa kolme asiaa: laskentatehoa, kaistanleveys ja energia. Näihin vaikuttaa oleellisesti laitteiden pienuus, joka heikentää mahdollisesti niiden tietoturvallisuutta. Tuenin mukaan turvallisuuden puute ei johdu kehittäjien välinpitämättömyydestä, vaan tietämättömyydestä. Hänen mukaansa valmistajat luottavat liikaa siihen, että heidän tuottamiaan laitteita käytetään vain yksityisissä verkoissa, ja että käyttäjä huolehtii laitteen tietoturvallisuudesta. Tämän vuoksi laitteet on suunniteltu siten, että kaikilla verkossaolijoilla on oletusarvoisesti pääkäyttäjän oikeudet. Tälläisiin tuotteisiin sisältyy suuria tietoturvariskejä, mikäli niitä käytetään

julkisissa langattomissa verkoissa, jolloin kuka tahansa voi käyttää laitetta. Valmistajat päätyvät myös usein käyttämään teollisen Internetin sovellutusten tuottamiseen kokemuksen pohjalta tuttua, mutta vanhentunutta tekniikkaa, koska uusien tekniikoiden käyttöönotto on kallista ja hidasta. Vanhentuneeseen tekniikkaan sisältyy usein tietoturvariskejä, jotka olisivat vältettävissä ahkeralla tekniikoiden päivittämisellä.

Tuenin työssään tutkimissa laitteissa oli laitteen sijainnin seurantaan liittyviä yksityisyyttä rikkovia tietoturva-aukkoja. Sijainnin paikantaminen oli esimerkkilaitteissa koettu tärkeäksi, joten sitä ei koettu yksityisyyttä rikkovaksi vaan hyödylliseksi ominaisuudeksi. Mikäli teollisen Internetin ratkaisu tarvitsee toimiakseen käyttäjän paikkatietoja, on tärkeä määrittää kuinka tarkasti paikkatieto kerätään, jotta sovellutus on toimiva, eikä kuitenkaan loukkaa käyttäjän yksityisyyttä. Esimerkiksi karttapalvelujen tarvinnee tietää paikkatietoja satojen metrien ja minuuttien tarkkuudella. Mikäli tätä tarkennettaisiin metrien ja sekuntien tarkkuuteen, on vaarana, että rikotaan käyttäjän yksityisyyttä. Käyttäjän yksityiselämään liittyvän tiedon tallentaminen tutkimus- ja tuotekehitystarkoituksiin on toinen merkittävä eettinen kysymys. Esimerkiksi reittitietojen tallentaminen saattaisi antaa arvokasta lisätietoa tiesuunnitteluun, mutta tiedot on ehdottomasti kerättävä anonyymisti, jotta yksittäisiä reittitietoja ei voida yhdistää tiettyyn käyttäjään. Lisäksi käyttäjällä on oikeus tietää, mitä tietoja hänestä kerätään. Yksityisyyteen liittyvien eettisten linjavetojen suunnittelu vaatii usein eri alojen asiantuntijoiden yhteistyötä, jotta teknilliset ratkaisut saadaan sovitettua yhteiskunnan sosiaalisiin ja filosofisiin tarpeisiin. [22]

3.4 Hyökkäystyypit ja -pisteet

Suomalaisessa mediassa palvelunestohyökkäykset (denial of service, DoS) nousivat suuren yleisön tietoisuuteen Osuuspankin jouduttua kyseisen hyökkäyksen kohteeksi vuoden 2015 alkupuolella. Palvelunestohyökkäyksen on tarkoitus estää palvelun toiminta ruuhkauttamalla sitä. Hyökkääjä lähettää suuren määrän pyyntöjä, jolloin palvelu hidastuu käyttökelvottomaksi tai pahimmassa tapauksessa kaatuu kokonaan. Palvelunestohyökkäyksessä voi olla yksi tai useita hyökkääjiä. Usean hyökkääjän versiota kutsutaan hajautetuksi palvelunestohyökkäykseksi (distributed denial of service, DdoS). [23]

SYN-tulva on DoS-hyökkäyksen eräs muoto. Se hyväksikäyttää tiedonsiirtoyhteyden varmistavaa kolmiosaista kättelyä, jossa käyttäjä lähettää ensin SYN-pyynnön, palvelin

vastaa SYN-ACK kättelyllä ja käyttäjä viimeistelee kättelyn ACK-viestillä. SYN ja ACK ovat TCP/IP-protokollan merkkilippuja. ”SYN-pyyntö” viittaa tahdistuslippuun (syncronize flag) ja ”ACK-viesti” kuittauslippuun (acknowledge flag). SYN-tulva -hyökkäyksen tarkoituksena on tuottaa palvelimelle niin suuri määrä keskeneräisiä kättelyitä, että palvelin jumiutuu ja muiden käyttäjien palvelut estyvät. Tulvan keskeneräiset kättelyt syntyvät siitä, että hyökkääjä ei koskaan lähetä ACK-viestiä. [24]

ICMP-tulva (Internet control message protocol), joka tunnetaan myös Ping-tulvana, perustuu ICMP-protokollan Ping-komennon hyväksikäyttämiseen. Komentoa käytetään tiedustelemaan, onko kyseinen laite yhteydessä lähettäjään. Kyselyn lähettäminen on kevyttä, mutta vastaaminen hieman raskaampaa, joten vastaajakone rasittuu ja näin tukkeutuu. [25]

UDP-tulva (user datagram protocol, UDP) on monimutkaisempi tulvahyökkäys, joka myös perustuu nimensä mukaisesti oman protokollansa hyväksikäyttöön. Tulva lähettää suuren määrän UDP-paketteja uhrikoneen portteihin. UDP-paketit sisältävät IP-paketin tietoja sekä eheys- ja porttitietoja. [26]

Mies välissä -hyökkäys (man-in-the-middle attack) on hyökkäysmuoto, jossa kolmas osapuoli asettuu kahden muun väliin. Normaalitilanteessa palvelu tapahtuu asiakkaan ja palveluntarjoajan välillä salaisesti. Mies välissä kirjaimellisesti tunkeutuu kahden osapuolen väliin ja kierrättää kaiken tietoliikenteen oman koneensa kautta. Näin hyökkääjä näkee kaiken liikenteen ja voi halutessaan muokata ja vakoilla kulkevaa liikennettä.

Tekniikan toteutuksia usein helpottaa tunnistettavuus. Laitteilla on omat IP-osoitteet ja käyttäjä on kirjautuneena omilla käyttäjätunnuksillaan. Sybil-hyökkäyksen tarkoitus on rikkoa tätä yksilöllisyyttä. Sybil-hyökkääjä on tunnusomaisesti kuin kuka tahansa muu käyttäjä, eli hyökkääjällä on kaikki samat oikeudet kuin tavallisella käyttäjällä. Sybil-hyökkääjä kuitenkin käyttää oikeuksiaan väärin. Esimerkiksi Twitter-sivuston klikkausäänestyksen voi voittaa luomalla loputtoman määrän Twitter-tilejä. Sybil-hyökkäys voi saada IoT-järjestelmässä aikaan vääriä hälytyksiä tai tavallisen käyttäjän menettämään yksityisyytensä. [27]

Teollisen Internetin laitteet ovat usein langattomia ja akkukäyttöisiä. Akkukäyttöiset laitteet louhivat energiaa esimerkiksi valosta tai liikkeestä. Ehtymishyökkäys on akkukäyttöisiin laitteisiin suunnattu hyökkäys, jonka tarkoituksena on saada laite

kuluttamaan niin paljon energiaa, että sen energiavarannot ehtyvät ja laite menettää toimintakykynsä. Hyvin suunniteltu laite lataa itseään ja käynnistyy hetken kuluttua uudelleen. Käynnistyksen yhteydessä laite on kuitenkin haavoittuvainen palvelunestohyökkäyksille sekä muille ehtymisen jälkeisille hyökkäyksille (post-depletion attack). [28]

3.5 OWASP TOP 10 -listaus

OWASP (The Open Web Application Security Project) on ei-kaupallinen organisaatio, jonka tarkoitus on edistää ohjelmistoturvallisuutta. Organisaatio tuo julkisuuteen yleisiä epäkohtia ohjelmistoturvallisuudessa sekä tuottaa käytännön ratkaisuja. OWASP TOP 10 -listaus sisältää kymmenen tietoturva-aihetta, jotka on syytä ottaa huomioon ohjelmistoja ja järjestelmiä luodessa. Acharya ym. kehottavat kehittäjiä pitämään listausta muistilistana työssään. Listaus on teknisesti painottunut eikä ota kantaa eettisiin näkökohtiin. OWASP TOP 10 -listaus on julkistettu vuosina 2010 ja 2013, ja uusimman julkaisun on tarkoitus ilmestyä viimeistään vuonna 2017. Tämän työn kannalta ohjelmistoturvallisuuden listaus ei ole keskiössä, mutta teollisen Internetin laitetteiden kautta kulkevat tiedot päätyvät palvelimille, joissa niitä käsitellään listauksen piiriin kuuluvilla ohjelmistoilla. [29, 30, 31]

4 Tutkimuksesssa käytetyt ohjelmistot

4.1 Käyttöjärjestelmä Kali Linux

Kali Linux on Linux-käyttöjärjestelmäversio, jota käytetään tunnistamaan tietoturvauhkia. Kali Linux sisältää yli 600 työkalua eettiseen hakkerointiin [32]. Kyseessä on siis hyvin varusteltu turvallisuusorientoitunut käyttöjärjestelmä. Kali on hyvä väline nopeaan turvallisuustestaamiseen sekä kattavampaan tutkimukseen. Sitä on käytetty mm. pilvipalvelujen heikkouksien kartoittamiseen [33] sekä DoS-hyökkäyksien tutkimiseen [34].

Kali Linuxin työkalut on luokiteltu 13:n eri otsikon alle niiden käyttötarkoituksen mukaan: tiedonkeruu (Information Gathering), haavoittuvuusanalyysi (Vulnerability Analysis), langattomat hyökkäykset (Wireless Attacks), Internet-sovellukset (Web Applications), hyväksikäyttötyökalut (Exploitation Tools), oikeusopilliset työkalut (Forensics Tools), rasitustestit (Stress Testing), nuuskimis- ja huijaustyökalut (Sniffing and Spoofing), salasanan murtaminen (Password attacks), pääsynylläpito (Maintaining Access), takaisinmallinnus (Reverse Engineering), laitteiston hakkerointi (Hardware Hacking) ja raportointityökalut (Reporting Tools). Laajemmat ohjelmistot saattavat kuulua useampaan kategoriaan, mutta ne on luokiteltu päätarkoituksensa mukaisesti. [35]

Tiedonkeruu-otsikon alta löytyy työkaluja TCP/IP -osoitteiden ja isäntänimien (hostname) etsintään sekä osoitteen liikenteen tunnistamiseen tarkoitettuja ohjelmistoja. Näiden ohjelminen päätarkoitus on tutkia porttiliikennettä.

Haavoittuvuusanalyysi-otsikon ohjelmistojen päätarkoitus on etsiä haavoittuvuuksia. Useat ohjelmistot haavoittuvuusanalyysi-otsikon alla käsittelevät SQL-injektioita. Tämän hetkisen OWASP tietoturvakartoituksen mukaan injektiohyökkäykset ovat suurimpia tietoturvauhkia [36].

Langattomat hyökkäystyökalut keskittyvät tutkimaan langattomien teknologioiden haavoittuvuuksia. Ohjelmistoja löytyy bluetooth ja WiFi -yhteyksien seurantaan, kaappaamiseen, estämiseen ja salasanojen murtamiseen.

Internet-sovellus -otsikon alta löytyy työkaluja kaikkiin OWASP TOP 10 -tietoturvakartoituksen turvallisuusuhkiin. Mikäli ohjelmisto on luokiteltu haavoittuvuusanalyysin sijaan Internet-sovelluksiin, on sen käyttötarkoitus tutkia

Internet-käyttöliittymää, kun vastaava työkalu haavoittuvuusanalyysi-otsinkon alla keskittyy tietokantaan tai tietokantakomentoihin. OWASP-listauksessa olevia Cross-site Scripting (XSS) ja Cross-Site Request Forgery (CSRF) -hyökkäyksiin keskittyviä ohjelmistoja löytyy paljon Internet-sovellus -otsikon alta.

Hyväksikäyttötyökalut sisältävät palvelimiin kohdistuvia toimenpiteitä ja shell-koodin käyttöä. Työkalujen päätarkoitus on päästä palvelinkoneelle, joka on usein Linux-pohjainen shell-kieltä tukeva kone, ja ajaa haitallisia koodeja. Nämä työkalut osaavat upottaa esimerkiksi python-koodiin shell-pätkiä, jotka päätyessään palvelimelle ajetaan sellaisenaan.

Oikeusopilliset työkalut etsivät jotain hyvin yksityiskohtaista tiedostomuotoa, esimerkiksi binäärisiä levykuvia (binary disk image). Binäärisiä levykuvia käytetään sulautetuissa laitteissa laiteohjelmistojen asentamiseen. Nämä ohjelmistot voivat muokata levykuvaa omiin tarkoituksiinsa tai estää sen toimivuutta.

Rasitustestit-otsikko sisältää rasitus- ja tulvatesteihin tarkoitettuja työkaluja. Nämä työkalut tuottavat haluttuun kohteeseen luonnottoman suuria kuormia, jotta nähdään millaisia kuormia kohde kestää.

Nuuskimis- ja huijaustyökalut ovat läheistä sukua tiedonkeruutyökaluille. Niillä seurataan verkkoliikennettä, mutta sen lisäksi niillä voidaan luoda huijausosoitteita ja -tietoa. IP-osoitehuijauksissa (IP spoofing) käytetään jonkun toisen olemassa olevaa IP-osoitetta tai luodaan väärennetty osoite.

Salasanan murtaminen -otsikon alta löytyy salasanan murtamiseen tarkoitetuja työkaluja. Murrettaessa salasanoja käytetään tunnetuimpia salasanoja, oletusarvoisia salasanoja tai raakaa voimaa. Salasanojen murtamiseen on myös kehitetty hienostuneempia salauksenpurkukirjastoja. Oletus salasanojen murtaminen on usein suosittua, koska niiden avulla saadaan suurimmat oikeudet hyökkäyskohteesta.

Pääsynylläpito-työkalut ovat takaporttien avaamista ja aukipitämistä varten. Murtautumisen jälkeen reitti on pidettävä auki, jotta arvokasta tietoa ehditään siirtää mahdollisimman paljon tai myöhempänä ajankohtana.

Takaisinmallinnustyökalut ovat läheistä sukua debuggaukseen tarkoitettujen ohjelmistojen kanssa. Niiden tarkoitus on kulkeutua kaikkiin testattavan ohjelman haaroihin ja etsiä puutteita tai vuotoja. Niiden avulla havaitaan muistivuotojen

mahdollisuuksia, vähän käytettyjä kirjastoja tai funktioita sekä kattavuuksia. Näiden avulla pahansuopa käyttäjä saa hyvän mallin ohjelmiston rakenteesta ja voi joko hyökätä sitä vastaan tai myydä sitä kopiona eteenpäin.

Laitteiston hakkerointi -osion työkalut kattavat Anrdoid- ja sulautettuihin laitteisiin suunnattuja työkaluja. Niiden avulla voidaan lukea tietoa laitteesta ja mahdollisesta ohjelmistosta.

Raportointityökalut sisältävät työkaluja tiedostomuotojen tutkintaan sekä kerätyn tiedon kuvalliseen esittämiseen. Nämä eivät varsinaisesti ole hyökkäymiseen tarkoitettuja työkaluja, vaan ne on tarkoitettu hyökkäysten tulosten tarkasteluun. [35]

4.2 Käyttöjärjestelmä Raspbian

Raspbian on Debianiin pohjautuva käyttöjärjestelmä, joka on muokattu toimimaan Raspberry Pi:llä. Raspbian tukee Raspberry Pi:n rakennetta ja näin nopeuttaa sen toimintaa. Raspberry Pi:n edistyksellinen rakenne käyttäälaskentaan liukulukuja kun perinteinen elektroniikka vastaavasti käyttää kokonaislukuja. Rasbian sisältää valmiiksi tuettuja ohjelmistoja, paketteja sekä helppokäyttöasetuksia. On kuitenkin muistettava, että Rasbian ei ole Raspberry Pi:n organisaation vaan käyttäjien kehittämä. [37, 38]

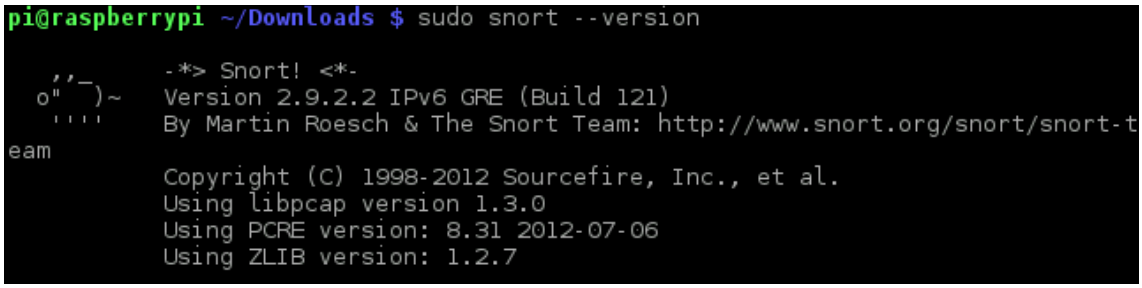
Fengin ym. tutkimuksen mukaan Raspbian-käyttöjärjestelmä sisältää kaksi merkittävää tietoturvariskiä. Käyttöjärjestelmän käyttäjänimi ja salasana on ennaltamääritetty. Käyttäjänimi on oletusarvoisesti pi ja salasana on oletusarvoisesti raspberry. Näiden muuttaminen on erityisen suositeltavaa, mikäli laitetta on tarkoitus käyttää Internetissä. Lisäksi etäyhteysportti 22 on oletusarvoisesti avoinna, mikä mahdollistaa etäyhteyden laitteeseen. Portin olisi syytä olla suljettuna, mikäli sitä ei tarvita aktiivisesti. Nämä kaksi tietoturvariskiä mahdollistavat oletusarvoisten laitteiden kaappaamisen ja käytön vahingollisesti. Fengin ym. mukaan nmap -verkon tutkimuskomento ei palauta Raspbian-käyttöjärjestelmää, joten Raspbian-laitetta on vaikeampi havaita verkosta. Tämä on kuitenkin pieni lisäturva ja mahdollisesti ohimenevä ilo verrattuna kahteen suureen tietoturvariskiin. Feng ym. ovat kuitenkin vakuuttuneita siitä, että Raspberry Pi on hyvä laite teollisen Internetin tuottamiseen. [39]

4.3 Tunkeilijan havaitsemisjärjestelmä Snort

Koska tietoturva on laaja ja monimuotoinen käsite, tietokoneen turvallisuutta voidaan parantaan monella taholla. Yleisesti tunnettuja keinoja ovat virustorjunta ja palomuuri.

Tässä työssä ei käsitellä virustorjuntaa, vaan keskitymme tutkimaan tunkeilijan havaitsemista ja torjumista. Verkkotunkeilijan havaitsemisjärjestelmän (network intrusion detection system, NIDS) avulla havaitaan vihamielisiä käyttäjiä sekä heidän tekemiään hyökkäyksiä. Tässä työssä laitteiston puolustamiseen käytettiin Snort-ohjelmaa, joka on tunnettu avoimeen lähdekoodiin perustuva verkontunkelijan havaitsemisjärjestelmä. Snortin vahvuuksiin lukeutuu sen keveys, joustava havainnointi sekä kattava ylläpito. Salah ja Kahtanin mukaan Snort:ia pidetään suuressa arvossa ja se on käytännössä vakiintunut käytäntö [40]. Kuvassa 2 on esitetty tässä työssä käytetyn ohjelman versio.

Snort-havaitsemisjärjestelmä on sääntöpohjainen. Esimerkkinä voisi olla tilanne, jossa toinen käyttäjä lähettää lähiverkosta pyynnön Raspberrylle, joka hyväksytään, jos käyttäjä on sallittujen listalla. Muutoin pyyntö evätään ja Snort ilmoittaa yhteydenottoyrityksestä ylläpitoon. Toisena esimerkkinä voisi olla tilanne, jossa käyttäjä ottaa yhteyden sivustolle Facebook.com, jolloin Snort lähettää ylläpitäjälle ilmoituksen ”Työntekijä Facebookkaa”. Vaikka Snort on yleistynyt käytäntö turvallisuuden parantamiseksi, sen on todettu olevan heikko palvelunestohyökkäyksille. Hyökkäyksen tuottamalla suurella pakettimäärillä Snort ylikuormittuu ja järjestelmässä alkaa esiintyä tietovuotoja. Tämä johtuu sääntöpohjaisuudesta, jossa yksiselitteiset säännöt eivät välttämättä kata tuhansien satunnaisten yhteydenottojen vaihtelua, eikä ohjelma ehdi arvioida riittävän tarkasti jokaista yhteydenottoa erikseen. [40, 41, 42]



Kuva 2: Snort versio

4.4 Palomuuri Iptables

Palomuuri on ohjelma tai lisälaite, joka asennetaan tietokoneeseen poistamaan pahantahtoista verkkoliikennettä. Kaikki verkkoliikenne liikkuu asennuksen jälkeen palomuurin kautta. Palomuuri suodattaa vain halutut paketit laitteelle ja estää

epäilyttävien pakettien läpipääsyn. Iptables-palomuuri on Linux-käyttöjärjestelmän sisäänasennettu paketinhallintaohjelma, jota voidaan käyttää pakettien seurantaan ja suodattamiseen. Iptables toimii sille asetettujen sääntöjen mukaan. Sääntöjen mukaiset paketit hyväksytään tai hylätään tarkoituksen mukaisesti. [43]

4.5 Kuvan- ja äänentoisto-ohjelma VLC

VLC on avoimeen lähdekoodiin perustuva kuvan- ja äänentoisto-ohjelma, joka toistaa videotiedostoja, levyjä ja nettikameralähetyksiä. Sitä voidaan käyttää myös suoratoiston välittämiseen. Suoratoisto (streaming), on tiedonsiirtomuoto, jossa ääntä ja videokuvaa (multimedia) tallennetaan ja lähetetään toisten osapuolten seurattavaksi reaaliajassa, vaikkei koko tallenne ole vielä valmis tai ladattu kokonaan. [23] VLC tukee kaikkia tunnetuimpia toistoalustoja sekä tallennusmuotoja. VLC on ladattavissa tietokoneille sekä mobiililaitteille, ja se tukee Android, iOS sekä Windows käyttöjärjestelmiä. [44, 45]

Tässä työssä käytimme VLC:tä tallentamaan, välittämään ja toistamaan reaaliaikaista kuvaa. Työssä ei tutkittu VLC:n ominaisuuksien vaikutusta turvallisuuteen. VLC valittiin toisto-ohjelmaksi lähinnä sen tunnettavuuden ja yksinkertaisuuden vuoksi. Se on todennäköinen valinta yksinkertaisesti ja nopeasti toteutetussa teollisen Internetin sovelluksessa. [45] VLC:n suoratoisto käyttää suoratoistoprotokollaa (real time streaming protocol, RTSP) [46]. Suoratoisto protokolla toimii TCP:n päällä samalla tavalla kuin hypertekstin siirtoprotokolla (hypertext transfer protocol, HTTP). HTTP:tä käytetään Internetselaimen toiminnassa.

4.6 TCP/IP-pakettien hallintatyökalu Hping3

Hping on TCP/IP-pakettien lähetys- ja analysointityökalu, jonka on kehittänyt italialainen avoimen lähdekoodin kehittäjä Sanfilippo Salvatore. Sillä voidaan tutkia TCP/IP-haavoittuvaisuuksia luomalla hyökkäyksiä. Hping on saavuttanut korkean aseman TCP/IP-tutkimuksessa ja kuuluu nykyään Kali-Linuxin vakiotyökaluihin. [47] Tässä tutkimuksessa käytimme ohjelman uusinta versiota, Hping3:a.

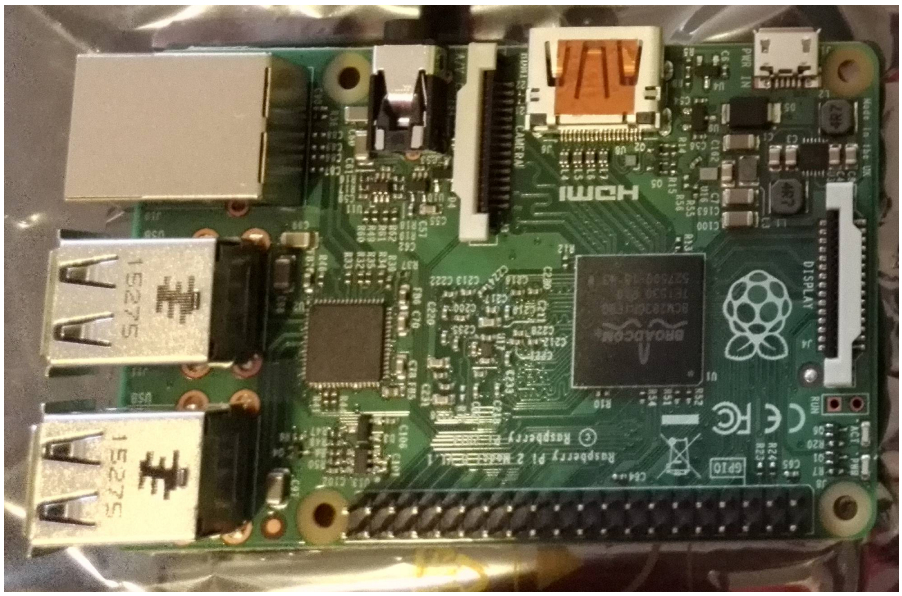
5 Kaluston valmistelu

5.1 Kalusto

Tutkimuksessa käytetty kalusto koostuu Raspberry Pi 2 Model B 1 GB:stä, Raspberry Pi:n kamerakortista, Wi-Pi WLAN-moduulista, Kingston 16 GB muistikortista, USB-laturista sekä Raspberry Pi:n kotelosta (kuva 3).

Kuva 3: Tutkimuksessa käytetty kalusto. Vasemmalta oikealle: Raspberry Pi 2 Model B 1 GB, Kamera, Wi-Pi, muistikortti, laturi, kotelo

Raspberry Pi on tämän hetken suosituimpia laitteita teollisen Internetin rakentamiseen (kuva 4). Raspberry Pi on karsittu tietokone, joka koostuu yhdestä ainoasta piirilevystä. Laitteessa ei ole varsinaista käyttöliittymää, näyttöä tai näppäimiä joilla vuorovaikuttaa laitteen toimintaan. Toisaalta Rasberry Pi:hin voi kytkeä käytännössä kaikkea, mitä tietokoneeseenkin, esimerkiksi useita USB-laitteita, verkkokaapelin, HDMI-laitteen (high-definition multimedia interface) tai muistikortin. Tässä tutkimuksessa käytetyn Raspberry Pi 2:n tuotetiedot löytyvät liitteestä A. [48]



Kuva 4: Raspberry Pi

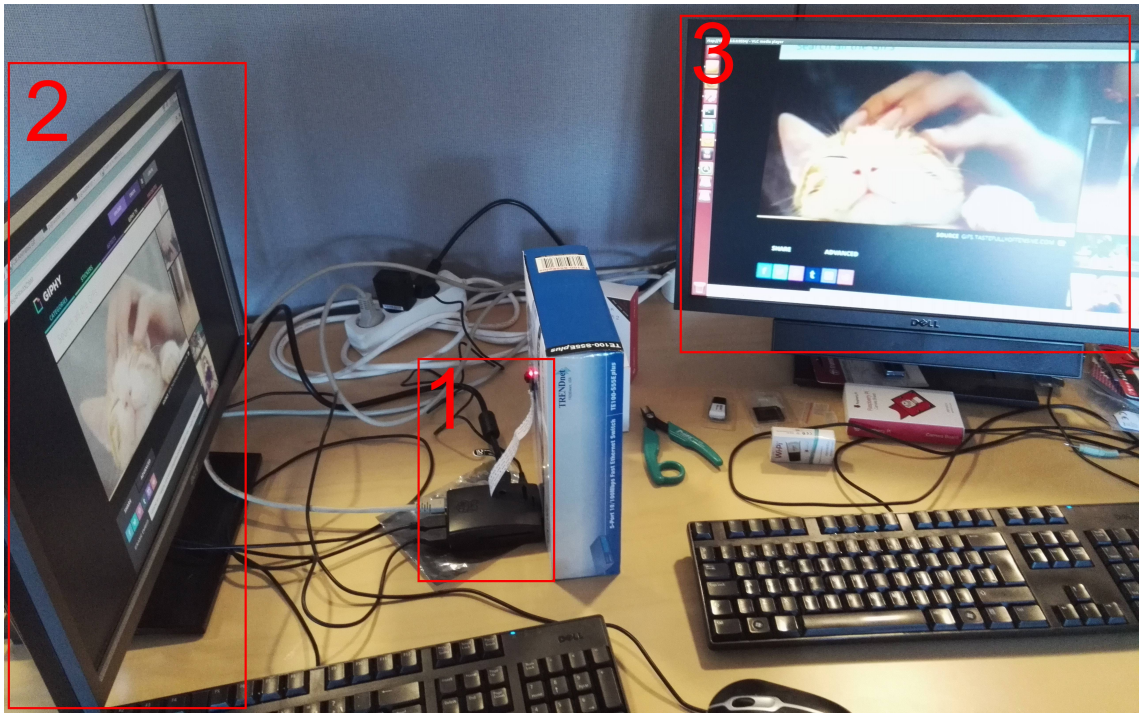
5.2 Raspberry Pi:n valmistelu

Tämän työn tarkoitus on etsiä haavoittuvaisuuksia yksinkertaisesti toteutetuista teollisen Internetin laitteista, joten Rasberryn Pi valmisteltiin testauksia varten mahdollisimman yksinkertaisesti. Arvioimme, että tavalliselle Raspberry Pi:n käyttäjälle toimivuus ja nopea ja helppo käyttöönotto ovat ensisijaisia asioita, jolloin turvallisuusseikat saattavat jäädä tarkistamatta tai kokonaan huomioimatta. Todellista käyttäjätilannetta mukaillaksemme käytimme valmistelussa Internetistä helposti löytyviä ohjeita ja Youtube-videoita.

Raspberryn valmistelu aloitettiin käyttöjärjestelmän asentamisella. Tässä työssä käytettiin käyttöjärjestelmänä Rasberry Pi:n kotisivuilta löytyvää Raspbian Wheezyä (versio: Toukokuu 2015, julkaisupäivä: 2015-05-05, ydinversio: 3.18) [49]. Käyttöjärjestelmän asennus muistikortille tapahtui Win32 Disk Imager-ohjelman avulla. Järjestemän käyttöönotto tapahtui Youtube-videota seuraten [50]. Tämän jälkeen kameran toimintakuntoon saattaminen tapahtui niin ikään Youtube-videon avulla [51].

Järjestelmä kasattiin Jyväskylän yliopiston Tietotekniikan laboratiorioon. Järjestelmä muodostuu Raspberry Pi:stä, Linux-tietokoneesta sekä SMC Barricade 7004AWBR-reitittimisestä. Raspberry Pi:lle asetettiin staattinen ip-osoite sen tunnistettavuutta varten, sekä mahdollistamaan yksinkertainen suoratoisto [52]. Verkkoasetusten jälkeen Raspberry Pi oli valmis lähettämään suoratoistokuvaa verkkoon. Lähettäminen ja

vastaanottaminen tapahtuu muutamalla yksinkertaisella komennolla [53]. Suoratoiston aloittaminen Raspberry Pi:llä tapahtui komennolla: ”raspivid -rot 180 -o - -t 0 -n -w 600 -h 400 | cvlc -vvv stream:///dev/stdin –sout '#rtp{sdp=rtsp://:8554/}' :demux=h264”. Vastaanottaja voi aloittaa suoratoiston katselun komennolla: ”vlc rtsp://192.168.0.6:8554/”, jossa 192.168.0.6 on Raspberry Pi:n IP-osoite. Kuvassa 5 on esitetty laboratorioon koottu suoratoisto-asetelma.



Kuva 5: Suoratoisto-asetelma: Kuvassa keskellä (1) on Raspberry Pi sekä kamera, joka on suunnattu kohti lähetettävää videota, kuvassa vasemmalla (2) on näyttö, jossa pyörii suoratoistettava video, kuvassa oikealla (3) on samassa lähiverkossa oleva tietokone, joka seuraa suoraa lähetystä.

6 Menetelmät

Tutkivan osan tarkoituksena oli tutkia Raspberry Pi:n haavoittuvuutta yleisesti tunnettujen hyökkäysten osalta sekä mahdollisesti parantaa sen tietoturvallisuutta.

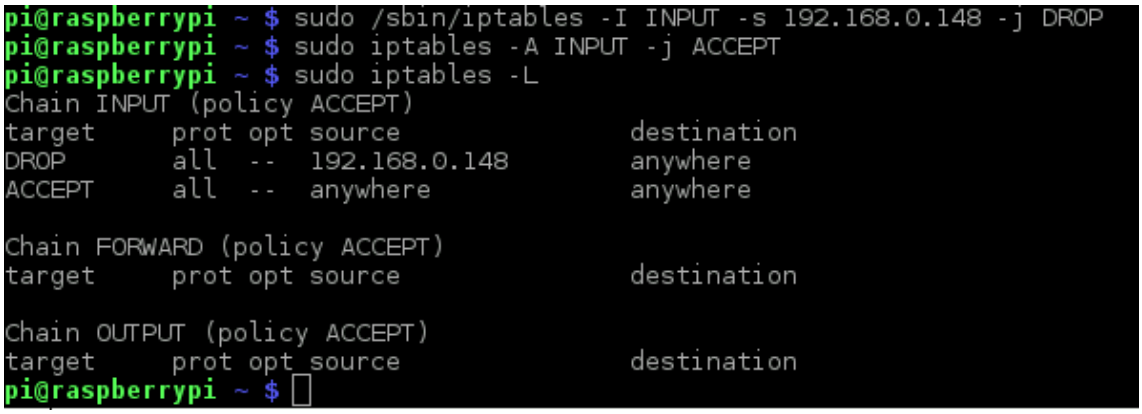
6.1 Hyökkäys

Tutkimuksesa tehtiin DoS-hyökkäyksiä, johon käytettiin TCP/IP-turvallisuustutkimuksiin tarkoitettua Hping3-ohjelmaa [54, 55]. Hyökkäykset toteutettiin kahdella erilaisella lähiverkolla, ensin Ethernet-lähiverkossa ja sitten WLAN-yhteyden yli [56]. Hyökkäyksiä tehtiin rajoitettuina sekä rajoittamattomina. Testasimme tutkimuksessa pakettien koon ja lähetysaikavälin vaikutusta puolustukseen.

6.2 Hyökkäyksen torjunta ja turvallisuuden parantaminen

Onnistuneiden hyökkäysten jälkeen Raspberry Pi:hin asennettiin Snort. Tarkoituksena oli testata Snortin tehokkuutta hyökkäyksen estämisessä ja havaitsemisessa. Snortiin asetettiin säännöksi, että kotiverkon ulkopuoliset kutsut pitää hylätä. Kotiverkkona olivat tässä tapauksessa Raspberry Pi ja suoratoistoa katseleva tietokone.

Epäonnistuneen puolustautumisen vuoksi päätettiin Raspberryyn Pi:hin asentaa Iptables-palomuuri. Ensimmäisessä kokeessa palomuuria käskettiin pysäyttämään kaikki liikenne hyökkääjäkoneelta Raspberry Pi:lle (kuva 6). Mirzaie ym. ovat tutkineet SYN-tulvalta suojautumista rajoittamalla sisään tulevia pakettaja [43]. Tästä johdettiin toinen kokeemme, jossa testasimme rajoittamista seuraavanlaisella komennolla: ”-A FORWARD -p tcp --syn -m limit --limit 1/s -j ACCEPT”.



Kuva 6: Iptables-palomuuri rajoittaa kaiken liikenteen Kali-hyökkääjältä (192.168.0.148) Raspberryyn

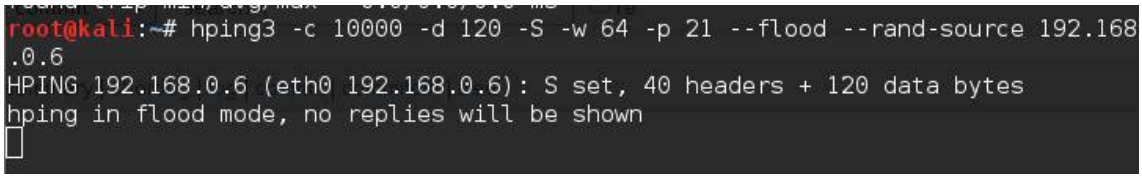
6.3 Vertailuarvot

Tehdyissä testeissä tulva pääsi vastoin ennakko-odotuksia tunkeutumaan puolustusohjelmien läpi. Läpipääsyn syyn selvittämiseksi Raspberry Pi:lle ja Kali-hyökkääjälle päätettiin määrittää vertailuarvo (benchmark) Sysbench-ohjelmalla. Sysbench on vertailutyökalu, joka tekee vertailukelpoisia toimintoja, esimerkiksi laskee alkulukuja 10000:een asti ja mittaa siihen kulunutta aikaa. Laitteille tehtiin yhden ja neljän langan (thread) vertailutestit. Lanka on tietotekniikassa käytetty termi, joka viittaa yksittäiseen erilliseen toimenpiteeseen.

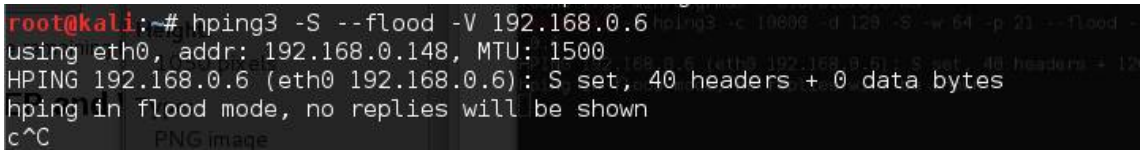
7 Tulokset

7.1 Hyökkäyksen vaikutuksia

Ensimmäinen hyökkäys rajoitetulla pakettimäärällä ja pakettien koolla sai videokuvan katkeamaan (kuva 7). Toinen hyökkäys täysin rajoittamatta sai aikaan videokuvan katkeamisen sekä hidasti Raspberry Pi:tä niin paljon, että sen käyttäminen oli mahdotonta (kuva 8). Raspberry Pi ei kaadu tai sammu, mutta sen ajamat ohjelmat pysähtyvät, eivätkä hiiri ja näppäimistö vastaa. Hyökkäyken loputtua Raspberry Pi käsittelee jäljellä olevat kutsut ja jatkaa toimintaansa normaalisti.



Kuva 7: Hyökkäys rajoitetulla pakettimäärällä sekä -koolla Hping3:n avulla



Kuva 8: rajoittamaton hyökkäys Hping3:n avulla

7.2 Snort tulokset

Vastoin odotuksia rajoittamaton hyökkäys meni lähes suodattamatta läpi. Testiajojen perusteella Snort pystyi pysäyttämään vain alle 30 % saapuvista hyökkäyspaketeista (Kuva 9).

```
===================================================
Packet I/O Totals:
   Received:          9998
   Analyzed:          6319 ( 63.203%)
    Dropped:          3679 ( 26.899%)
   Filtered:             0 (  0.000%)
Outstanding:          3679 ( 36.797%)
   Injected:             0
===================================================
```

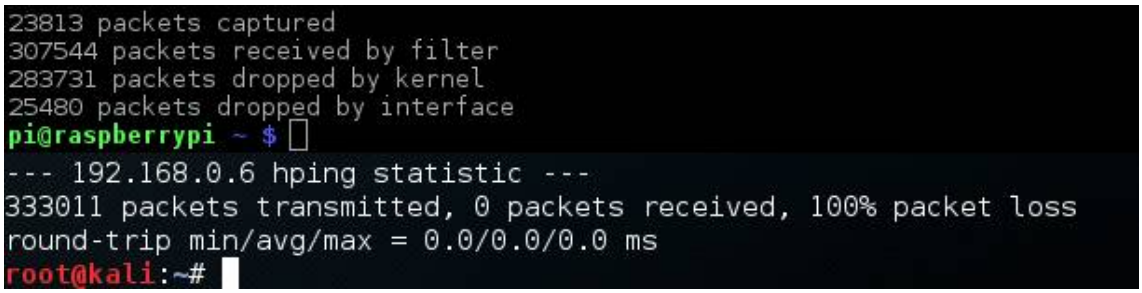
Kuva 9: Snortin tulos Hping3-hyökkäykselle

Snortin antama tulos ei kuitenkaan kerro kaikkea tapahtuneesta. Hpingin tilastot paljastavat läpi menevien pakettien määrän olevan huomattavasti suurempi. Kuvasta 10 nähdään Hpingin lähettäneen 3 226 602 pakettia noin minuutin kestäneessä testissä. Niistä vajaa 10 000 päätyi Snortin käsittelemiksi, ennen kuin Raspberry Pi lopetti toimintansa. Snortin toiminta ei pystynyt juurikaan hidastamaan rajoittamattoman hyökkäyksen kulkua.

Kuva 10: Hping:n tilasto

7.3 Iptables tulokset

Iptables pystyi estämään sekä yksittäisen ping-pyynnön että rajoitetun hyökkäyksen. Yllätykseksemme se ei kuitenkaan pysäyttänyt rajoittamatonta Hping-hyökkäystä. Kuvassa 11 on esimerkkinä yksi rajoitettu hyökkäys, jonka Iptables pystyy estämään.



Kuva 11: Kuvassa ylhäällä Iptablesin käsittelemät paketit ja alhaalla Hping3:n lähettämät paketit

Mirzaie ym. tekemän tutkimuksen mukaisesti saapuvien pakettien rajoittamista sovellettiin Raspberry Pi:n palomuuriin usealla variaatiolla [43,57,58], mutta se ei ollut riittävä estämään rajoittamatonta SYN-hyökkäystä.

7.4 Rajoitetut hyökkäykset: pakettikoon ja pakettien lähetysten aikavälin vaikutus puolustukseen

Tulokset voidaan jakaa kolmeen alueeseen: hyökkäys ei vaikuta havaittavasti, hyökkäys estää käytön täysin, sekä välimaastoon. Tässä tapauksessa välimaaston tunnistaa siitä,

että suoratoistettu video katkeaa, mutta Raspberry Pi jatkaa toimintaansa normaalisti.

Pakettikoon testaaminen on hyökkääjän näkökulmasta turhaa, koska SYN-tulvassa lähetetään normaalisti nollan tavun kutsuja, ja pakettikoon lisääminen vain heikentää hyökkäystä. Pakettikoon testaaminen kuitenkin osoittaa, millaisia määriä ”oikeita” paketteja Raspberry Pi kestää. Täydellinen estyminen tapahtui alle 55 tavun pakettikoolla. Yli 109 tavun pakettikoolla Raspberry Pi:n toiminnassa ei tapahtunut mitään havaittavaa muutosta. Välimaasto sijoittuu 55 - 109 tavun koon välille.

Pakettien lähetysten aikavälin testaaminen vastaa todellisen hyökkääjän haasteita. Kohteeseen päätyvien hyökkäysten määrä voi vaihdella riippuen hyökkäyslaitteen tehosta tai verkon nopeudesta. Mikäli lähetettävien kutsujen aikaväli on yli 16 mikrosekunttia, ei hyökkäys vaikuttanut Rasperry Pi:n toimintaan havaittavasti. Täydellinen estyminen saavutettiin vasta rajoittamattomalla hyökkäyksellä. Pelkkä videokuvan katkeaminen saatiin aikaan pakettien välisen aikavälin ollessa 1 – 16 mikrosekunttia. Tämä välimaasto on hyökkääjän näkökulmasta mielenkiintoisin. Se ei näy Raspberry Pi:n käyttäjälle, jollei sitä aktiivisesti etsitä, mutta suoratoisto katkeaa. Täysin rajoittamaton hyökkäys paljastuu helpommin. Välimaasto on näin ollen edullisin vaihtoehto toiminnan estämiseksi.

7.5 Vertailuarvo

Sysbenchin tulokset on esitetty taulukossa 1. Vertailuarvot löytyvät kokonaisuudessaan liitteinä (Liite 8.2 ja 8.3). Tuloksista huomataan Kali-hyökkääjän olevan huomattavasti nopeampi molemmista testeissä.

Taulukko 1: Sysbench-vertailutestin tulokset

Laite \ Testi	Yhden langan vertailutesti	Neljän langan vertailutesti
Raspberry Pi	783.4252 s	198.9062 s
Kali-hyökkääjä	21.5243 s	12.5200 s

8 Yhteenveto ja pohdinta

Tutkimuksessa oli alunperin tarkoitus tutkia useita hyökkäystyyppejä ja nopeita ratkaisuja teollisen Internetin suojaamiseen niiltä. Raspberry Pi:n suojaaminen SYN-tulvalta osoittautui kuitenkin niin haastavaksi, että keskityimme siihen. Testien ja aiheesta julkaistujen tutkimusten välillä on kuitenkin ristiriitaa. Tutkimukset antavat selkeitä tuloksia ja menetelmiä, joilla SYN-tulva on onnistuttu torjumaan. Meidän tutkimuksessamme sen sijaan ei onnistuttu torjumaan kyseisiä hyökkäyksiä tutkimuksissa kuvatuilla menetelmillä.

Sysbenchin tulokset osoittavat Kali-hyökkääjän olevan 35 kertaa nopeampi yhden langan vertailutestissä ja 15 kertaa nopeampi neljän langan vertailutestissä. Näin suurta nopeuseroa voidaan pitää syynä puolustautumisen epäonnistumiseen. Raspberry Pi ei ehdi pudottaa saapuvaa liikennettä sitä tahtia, kuin liikennettä syntyy lisää.

Tehdyissä testeissä rajoitettujen hyökkäysten annettiin vaikuttaa Raspberry Pi:hin alle kahden minuutin ajan. Estymisrajat saattaisivat olla erilaiset kuin tässä kokeessa havaittiin, jos altistumisaika olisi pidempi. Estymisrajat riippuvat myös Raspberry Pi:n omasta kuormituksesta, ja eri koneyksilöiden välillä saattaa myös olla vaihtelua. Tässä kokeessa havaitut estymisrajat antavat kuitenkin viitettä siitä, millaista rasitusta Raspberry Pi kestää. Tutkimuksen aikana on julkaistu uusi sukupolvi Raspberry Pi:stä, Raspberry Pi 3. Kyseinen laite sisältää sisäänrakennettut WLAN ja Bluetooth -moduulit ja 1,2 GHz prosessorin. Prosessointitehon kasvu on kuitenkin suhteellisesti niin vähäinen, että hyökkäykset pystyvät ylikuormittamaan myös uuden sukupolven Raspberry Pi:n, joskin jumiutumisen raja-arvot saattavat olla uuden sukupolven laitteessa hieman erilaiset.

Teollisen Internetin laitteet ovat usein yksinkertaisia, pieniä ja itsenäisiä. Niille on tärkeää vähäinen virrankulutus sekä tarkoitukseen riittävä laskentateho. Tämä tutkimus osoittaa niiden olevan kuitenkin haavoittuvaisia palvelunestohyökkäyksille. Mikäli hyökkääjä pääsee samaan lähiverkkoon teollisen Internetin laitteen kanssa, on laite palvelunestohyökkäyksille alttiina, vaikka laitteeseen olisi asennettu turvajärjestelyjä. Yksittäisen laitteen haavoittuvuutta voitaisiin luultavasti parantaa suunnittelemalla teollisen Internetin verkko hyvin. Julkisten WLAN-reitittimien käyttö ei ole teollisen Internetin käytössä suositeltavaa. Turvallisempi vaihtoehto olisi esimerkiksi kierrättää laitteiden lähettämät tiedot vartavasten asennetun hyvin suojatun palvelimen kautta.

9 Lähdeluettelo

[1] http://vnk.fi/artikkeli/-/asset_publisher/tutkimus-suomesta-teollisen-internetin-piilaakso

[2] http://www.tekniikkatalous.fi/tyoelama/viime-vuonna-potkut-sai-11-907-tyontekijaa-yt-neuvottelujen-piirissa-114-000-6243334

[3] A. Butowsky, K. Gai, M. Coakley, M. Qiu, C. C. Tappert, ”City of White Plains Parking App: Case Study of a Smart City Web Application”, IEEE 2nd International Conference on Cyber Security and Cloud Computing, 2015

[4] N. Wakaza, M. Loock, E. Kritzinger, ”A pragmatic approach towards the integration of ICT security awareness into the South African education system”, IEEE Conference Publications, s. 35-40, 2015

[5] D. Ross, ”Editor's letter,” Engineering & Technology **8,** 4p (2013).

[6] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, ”Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications”, Communications Surveys & Tutorials, p2347-2376, 2015

[7] V.G. Cerf, P.T. Kirsten, ”Gateways for the Internet of Things: An old problem revisited”. Global Communications Congerence (GLOBECOM), p2641-2647, 2013

[8] Sheeraz A. Alvi, Bilal Afzal, Ghalib A. Shah, Luigi Atzori, Waqar Mahmood, ”Internet of multimedia things: Vision and challenges,” Ad Hoc Networks Volume 33, 87-111 (2015)

[9] G. Sallai, ”Chapters of Future Internet research”, Cognitive Infocommunications (CogInfoCom), p161-166, Joulukuu 2013

[10] D. Evans, ”The Internet of things: How the next evolution of the Internet is changing everything”, CISCO, 2011

[11] Y. Upadhyay, A. Borole, D. Dileepan, ”MQTT Based Secured Home Automation System”, Symposium on Colossal Data Analysis and Networking, 2016

[12] S. Wagle, ”Semantic Data Extraction over MQTT for IoTcentric Wireless Sensor Networks, International Conference on Internet of Things and Application, 2016

[13] S. Rivera, Z. Fei, J. Griggioen, ”RAPTOR: A REST API TranslaTOR for OpenFlow Controllers, IEEE INFOCOM International Workshop on Computer and

Networking Experimental Research Using Testbeds, 2016

[14] L. Li, W. Chou, ”Designing Large Scale REST APIs Based on REST Chart”, IEEE International Conference on WEB Services, 2015

[15] Z. Yang, A. Li, L. Yu, S. Kang, M. Han, Q. Ding, ”An Improved AES Encryption Algorithm Based on Chaos Theory in Wireless Communication Networks, International Conference on Robot, Vision and Signal Processing, 2015

[16] P. Deshpande, S. Bhosale, ”AES Encryption Engines of Many Core Processor Arrays on FPGA by Using Parallel, Pipeline and Sequential Technique, International Conference on Energy Systems and Applications, 2015

[17] A. Alhamedi, H. Aldosari, V. Snasel, A. Abraham ”Internet of Things Communication Reference Model”, Computational Aspects of Social Networks, 2014

[18] H.C. Pohls, V. Angelakis, S. Suppan, K. Fischer, G. Oikonomou, E.Z. Tragos, R. Diaz Rodriguez, T. Mouroutis, ”RERUM: Building a reliable IoT upon privacy- and security enabled smart objects”, Wireless Communications and Networking Conference Workshops (WCNCW), p122-127, 2014

[19] Rolf H. Weber, ”Internet of Things – New security and privacy challenges”, Computer Law & Security Review, Volume 26, Issue 1, p23-30, January 2010

[20] Xu Teng, J. B. Wendt, M. Potkonjak, ”Security of IoT systems: Design challenges and opportunities”, Computer-Aided Design (ICCAD), 2014 IEEE/ACM International Conference, Marraskuu 2014

[21] Gou Quandeng, Yan Liashan, Liu Yihe, Li Yao, ”Construction and Strategies in IoT Security System”, Green Computing and Communications, p1129-1132, Elokuu 2013

[22] C. D. Tuen, ”Security in Internet of Things Systems”, Norwegian University of Science and Technology, 2015

[23] N. Altiparmak, A. Tekeoglu, A.S. Tosun, ”DoS resilience of real time streaming protocol”, Performance Computing and Communications Conference (IPCCC), 2011 IEEE 30th International, p1-8, 2011

[24] T. Nakashima, S. Oshima, ”A Detective Method for SYN Flood Attacks”, Innovative Computing, Information and Control, p48-51, 2006

[25] J. Udhayan, R. Anitha, ”Demystifying and Rate Limiting ICMP hosted DoS/DDoS

Floodin Attacks with Attack Productivity Analysis", Advance Computing Conference, p558-564, 2009

[26] S.S. Kolahi, K. Treseangrat, B. Sarrafpour, "Analysis of UDP DdoS flood cyber attack and defense mechanisms on Web Server with Linux Ubuntu 13", Communications, Signal Processing, and their Applications (ICCSPA), p1-5, 2015

[27] Zhang Kuan, Liang Xiaohui, Lu Rongxing, Shen Xuemin, "Sybil Attacks and Their Defenses in the Internet of Things", Internet of Things Journal, p372-383, 2014

[28] Xianghui Cao, Yu Cheng, Zequ Yang, Yang Zhou, Jiming Chen, "Ghost-in-ZigBee: Energy Depletion Attack on ZigBee based Wireless Networks", Internet of Things Journal, 2016

[29] https://www.owasp.org/index.php/Main_Page

[30] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[31] S. Acharya, B. Ehrenreich, J. Marciniak, "OWASP Inspired Mobile Security", Bioinformatics and Biomedicine (BIBM), 2015

[32] http://docs.kali.org/

[33] A. Durrani, "Analysis and prevention of vulnerabilities in cloud applications", Information Assurance and Cyber Security (CIACS) Conference, p43-46, 2014

[34] J.N. Goel, B.M. Mehtre, "Dynamic Ipv6 activation based defense for Ipv6 router advertisement flooding (DoS) attack", Computational Intelligence and Computing Research (ICCIC), p1-5, 2014

[35] http://tools.kali.org/tools-listing

[36] https://www.owasp.org/index.php/Top10#OWASP_Top_10_for_2013

[37] M. Sahani, S. K. Rout, A. K. Sharan, S. Dutta, "Real time color image enchancement with a high regard for restoration of skin color by using Raspberry Pi", Communications and Signal Processing (ICCSP), 2014 International Conference, Huhtikuu 2014

[38] https://www.raspbian.org/

[39] X. Feng, B. Onafeso, E. Liu, "Investigating Big Data Healthcare Security Issues with Raspberry Pi", Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive

Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015

[40] K. Salah, A. Kahtani, ”Improving snort performance under linux”, Communications, IET 3-12, p1883-1895, Joulukuu 2009

[41] A. Saboor, M. Akhlaq, B. Aslam, ”Experimental evaluation of Snort against DDoS attacks under different hardware configurations” Information Assurance (NCIA), 2013 2nd National Conference, p31-37, 2013

[42] N. Khamphakdee, N. Benjamas, S. Saiyod, ”Improving Intrusion Detection System based on Snort rules for network probe attack detection”, Information and Communication Technology (ICoICT), 2014 2nd International Conference, p69-74, 28-30.3.2014

[43] S. Mirzaie, A.K. Elyato, M.A. Sarram, ”Preventing of SYN Flood Attack with Iptables Firewall”, Communication Software and Networks ICCSN '10, p532-535, 2010

[44] http://www.videolan.org/vlc/index.html

[45] G. Munoz Ferrer, H. Meric, J.M. Piquer, J. Bustos-Jimenez, ”Performance evaluation of streaming algorithms for network cameras”, Computer Communications Workshops, p281-286, 2014

[46] Qun Yin, Jianbo Zhang, ”Development of remote video monitoring system based TCP/IP”, Computer Science & Education (ICCSE), p596-600, 2015

[47] http://tools.kali.org/information-gathering/hping3

[48] https://www.raspberrypi.org/

[49] https://www.raspberrypi.org/downloads/raspbian/

[50] https://www.youtube.com/watch?v=b6h95jNWg1g, ”SparkFun Getting Started with Raspberry Pi Part 1: Introduction”

[51] https://www.youtube.com/watch?v=T8T6S5eFpqE, ”Raspberry Pi - Camera Tutorial...”

[52] http://www.suntimebox.com/raspberry-pi-tutorial-course/week-3/day-5/

[53] http://www.raspberry-projects.com/pi/pi-hardware/raspberry-pi-camera/streaming-video-using-vlc-player

[54] http://www.hping.org/

[55] http://www.blackmoreops.com/2015/04/21/denial-of-service-attack-dos-using-

hping3-with-spoofed-ip-in-kali-linux/

[56] http://www.howtogeek.com/167425/how-to-setup-wi-fi-on-your-raspberry-pi-via-the-command-line/

[57] http://www.netfilter.org/documentation/HOWTO/packet-filtering-HOWTO-7.html

[58] http://blog.bodhizazen.net/linux/prevent-dos-with-iptables/

10 Liitteet

10.1 Liite A: Raspberry Pi 2 Model B 1GB-tuotetiedot

Raspberry Pi

Raspberry Pi 2, Model B

Product Name	**Raspberry Pi 2, Model B**
Product Description	The Raspberry PI 2 delivers 6 times the processing capacity of previous models. This second generation Raspberry PI has an upgraded Broadcom BCM2836 processor, which is a powerful ARM Cortex-A7 based quad-core processor that runs at 900MHz. The board also features an increase in memory capacity to 1Gbyte.
RS Part Number	**832-6274**
Specifications	
Chip	Broadcom BCM2836 SoC
Core architecture	Quad-core ARM Cortex-A7
CPU	900 MHz
GPU	Dual Core VideoCore IV® Multimedia Co-Processor
	Provides Open GL ES 2.0, hardware-accelerated OpenVG, and 1080p30 H.264 high-profile decode
	Capable of 1Gpixel/s, 1.5Gtexel/s or 24GFLOPs with texture filtering and DMA infrastructure
Memory	1GB LPDDR2
Operating System	Boots from Micro SD card, running a version of the Linux operating system
Dimensions	85 x 56 x 17mm
Power	Micro USB socket 5V, 2A
Connectors:	
Ethernet	10/100 BaseT Ethernet socket
Video Output	HDMI (rev 1.3 & 1.4)
	Composite RCA (PAL and NTSC)
Audio Output	3.5mm jack, HDMI
USB	4 x USB 2.0 Connector
GPIO Connector	40-pin 2.54 mm (100 mil) expansion header: 2x20 strip
	Providing 27 GPIO pins as well as +3.3 V, +5 V and GND supply lines
Camera Connector	15-pin MIPI Camera Serial Interface (CSI-2)
JTAG	Not populated
Display Connector	Display Serial Interface (DSI) 15 way flat flex cable connector with two data lanes and a clock lane
Memory Card Slot	Micro SDIO

RS

www.rs-components.com/raspberrypi

Kuva A.1: Raspbery Pi 2, Model B-tuotetiedot

10.2 Liite B: Raspberry Pi:n vertailuarvot Sysbench-testissä

pi@raspberrypi ~ $ sysbench --test=cpu --cpu-max-prime=20000 run

sysbench 0.4.12: multi-threaded system evaluation benchmark

Running the test with following options:
Number of threads: 1

Doing CPU performance benchmark

Threads started!
Done.

Maximum prime number checked in CPU test: 20000

Test execution summary:
   total time: 783.4252s
   total number of events: 10000
   total time taken by event execution: 783.3978
   per-request statistics:
        min: 78.00ms
        avg: 78.34ms
        max: 113.74ms
        approx. 95 percentile: 79.32ms

pi@raspberrypi ~ $ sysbench --test=cpu --cpu-max-prime=20000 --num-threads=4 run
sysbench 0.4.12: multi-threaded system evaluation benchmark

Running the test with following options:
Number of threads: 4

Doing CPU performance benchmark

Threads started!
Done.

Maximum prime number checked in CPU test: 20000

Test execution summary:
   total time: 198.9062s
   total number of events: 10000
   total time taken by event execution: 795.3715
   per-request statistics:
        min: 77.97ms
        avg: 79.54ms
        max: 141.50ms
        approx. 95 percentile: 82.84ms

10.3 Liite B: Kali-hyökkääjän vertailuarvot Sysbench-testissä

```
root@kali:~# sysbench --test=cpu --cpu-max-prime=20000 --num-threads=4 run
sysbench 0.4.12:  multi-threaded system evaluation benchmark

Running the test with following options:
Number of threads: 4

Doing CPU performance benchmark

Threads started!
Done.

Maximum prime number checked in CPU test: 20000


Test execution summary:
    total time:                          12.5200s
    total number of events:              10000
    total time taken by event execution: 50.0591
    per-request statistics:
         min:                            2.14ms
         avg:                            5.01ms
         max:                            32.29ms
         approx.  95 percentile:         14.15ms

root@kali:~# sysbench --test=cpu --cpu-max-prime=20000 run
sysbench 0.4.12:  multi-threaded system evaluation benchmark

Running the test with following options:
Number of threads: 1

Doing CPU performance benchmark

Threads started!
Done.

Maximum prime number checked in CPU test: 20000


Test execution summary:
    total time:                          21.5243s
    total number of events:              10000
    total time taken by event execution: 21.5230
    per-request statistics:
         min:                            2.14ms
         avg:                            2.15ms
         max:                            5.47ms
         approx.  95 percentile:         2.16ms
```