Aleksi Räsänen

ESINEIDEN INTERNETIN TIETOTURVAUHKAT TEOLLISUUDEN YRITYKSISSÄ

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2018

TIIVISTELMÄ

Räsänen, Aleksi
Esineiden Internetin tietoturvauhkat teollisuuden yrityksissä
Jyväskylä: Jyväskylän yliopisto, 2018, s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Seppänen, Ville

Esineiden Internetin käyttö on ollut pitkään nousussa ja se on muokannut yhteiskuntaamme monella tavalla. Myös teollisuus on hyödyntänyt Esineiden Internetin sovelluksia monella tasolla. Haittavaikutuksina on kuitenkin ilmennyt paljon erilaisia tietoturvauhkia, jotka ovat motivoineet tätä tutkielmaa. Tutkielma on suoritettu kirjallisuuskatsauksena ja sen tarkoituksena on selvittää teollisen Esineiden Internetin oleelliset tietoturvauhkat, niihin liittyvät haasteet ja ratkaisut. Tutkielmassa selviää, että teollisen Esineiden Internetin suuret verkot ja järjestelmät integroivat sisäänsä niin paljon erilaisia osioita, että niitä koskettaa suuri määrä perinteisiä tietoturvauhkia. Tämä verkkojen ja järjestelmien suuri koko ja heterogeenisyys aiheuttavat suuria haasteita vahvan tietoturvatason saavuttamiseksi. Haasteita aiheuttaa myös laitteiden pienet resurssit ja standardoinnin puute. Vahvojen tietoturvamekanismien implementoiminen on vaikeaa laitteisiin, joiden tietotekniset resurssit ovat pienet. Verkkojen laitteiden heterogeenisyys ja erilaiset standardit laitteissa sekä ohjelmistoissa johtavat myös usein tietoturva-aukkojen syntyyn. Ratkaisut on vielä kirjallisuuden mukaan tulevaisuuden tutkimuksen aiheena, mutta joitain ratkaisuja on jo kehitetty. Laitetason ratkaisuja on ARM TrustZone ja turvallisuusohjain, mutta myös henkilöstön koulutusta pidetään erittäin oleellisena ratkaisuna.

Asiasanat: Esineiden Internet, teollisuus, IoT, tietoturva, kerrosarkkitehtuuri, haavoittuvuus, hyökkäysrajapinta

ABSTRACT

Räsänen, Aleksi
Information security threats in industrial Internet of Things
Jyväskylä: University of Jyväskylä, 2018, pp.
Information Systems Science, Bachelor's Thesis
Supervisor: Seppänen, Ville

The use of Internet of Things (IoT) has been rising for a long time and it has shaped our society in many ways. Industry has also utilized the applications of IoT on many levels. There are numerous information security threats regarding industrial IoT which have motivated this study. This study is a literature review and it's goal is to examine industrial IoT's information security threats, challenges regarding them and solutions. Study shows that industrial IoT's big networks and systems integrate so many things in them that there is a substantial amount of information security threats regarding them. Heterogeneity and size of these networks and systems cause big challenges in order to achieve strong information security mechanisms. Lack of standardization and small size of devices also cause challenges. It's very challenging to implement strong information security mechanisms to devices that have little computing resources. Heterogeneity of networks and different standards on devices and programs also lead to vulnerabilities. According to literature, solutions are still yet to be researched in the future. Though there are some solutions developed already. ARM TrustZone and security controller are hardware-level solutions but proper training of employees is kept as a very relevant solution.

Keywords: Internet of Things, industry, IoT, information security, layer architecture, vulnerability, attack surface

KUVIOT

KUVIO 1 Esineiden Internetin sovelluksia & ominaisuuksia …….. 12
KUVIO 2 Kyberfyysisen tuotannonohjausjärjestelmän arkkitehtuuri ja hyökkäysrajapinnat ..…… 15

SISÄLLYS

TIIVISTELMÄ
ABSTRACT
KUVIOT

1 JOHDANTO……. 6

2 ESINEIDEN INTERNET - RAKENNE JA TEKNOLOGIAT…….. 8
2.1 Rakenteen kuvaus……..…. 8
2.2 Teknologiat…… 9
2.2.1 Radio Frequency IDentification…… 9
2.2.2 Near Field Communication……... 9
2.2.3 Sensoriverkot……... 9
2.3 Sovelluksia & ominaisuuksia……. 10
2.4 Esineiden Internet teollisuudessa…….. 13

3 TIETOTURVAUHKAT, HAASTEET JA RATKAISUT……. 14
3.1 Tietoturvauhkien muodot…….. 14
3.1.1 Havainnointikerros…….. 15
3.1.2 Kuljetuskerros……... 16
3.1.3 Käyttökerros…….. 17
3.1.4 Ihmiset…… 17
3.2 Haastet……... 18
3.3 Ratkaisut……..... 19

4 YHTEENVETO…… 20

LÄHTEET…… 23

1 JOHDANTO

Nykypäivän yhteiskunnassa teknologiaa implementoidaan jatkuvasti erilaisiin käyttötarkoituksiin ja se kehittyy erittäin nopeasti. Nopeassa kehityksessä jotkin asiat voivat kuitenkin jäädä hieman jälkeen ja näin voisi todeta tapahtuneen Esineiden Internetin tapauksessa. **Esineiden Internet eli Internet of Things (IoT)** rakentuu joukosta laitteita ja sensoreita, jotka mittaavat, käsittelevät ja jakavat informaatiota verkon ylitse eri alustoilla (Gubbi ym. 2013). Esineiden Internetin käyttö on yleistynyt teollisuudessa paljon ja se on tehnyt tuotantolaitoksista joustavampia ja kustannustehokkaampia. Sen soveltaminen on valitettavasti tuonut varjopuolena suuren määrän tietoturva-aukkoja ja haavoittuvuuksia, jotka altistavat teollisen Esineiden Internetin suurelle joukolle erilaisia tietoturvauhkia. Tämän tutkielman tarkoituksena on selvittää kirjallisuukatsauksena teollisen Esineiden Internetin yleisimmät tietoturvauhkat, löytää niihin liittyviä haasteita ja selvittää ratkaisuja. Vaikka teollisuudessa Esineiden Internetin sovelluksia on integroitu paljon, oli lähdemateriaalia haasteellista löytää haasteisiin ja ratkaisuihin. Tutkielmaan on valittu ratkaisuja, jotka ovat jo valmiita implementoitaviksi, sillä suurin osa ratkaisuista on vielä konseptuaalisella tasolla. Tutkielma vastaa kolmeen tutkimuskysymykseen:

- **Mitä tietoturvauhkia teolliseen Esineiden Internetiin liittyy?** Tarkoituksena selvittää yleisimpiä tietoturvauhkia, joita teollisen Esineiden Internetin eri osa-alueisiin liittyy. Tietoturvauhkat käydään läpi ja niiden toimintamekanismit käydään yleisellä tasolla läpi. Syvästi tekniselle tasolle ei voida mennä kandidaatin tutkielman rajoitteiden ja aiheen laajuuden vuoksi.

- **Mitä haasteita teollisen Esineiden Internetin tietoturvauhkiin liittyy?** Tutkielmassa selvitetään, mitkä ovat oleellisimpia haasteita teollisen Esineiden Internetin tietoturvauhkien ratkaisemisessa.

- **Mitä ratkaisuja on kehitetty teollisen Esineiden Internetin tietoturvauhkiin?** Tutkielmassa perehdytään olemassa olevia ratkaisuja teollisen Esineiden Internetin tietoturvauhkiin. Vasta kehitteillä olevia tai tutkimuksen kohteena olevia ratkaisuja ei tutkielmassa käsitellä.

Tutkielman aihepiiri on nykypäivänä tärkeä, sillä järjestelmät keräävät ja käsittelevät koko ajan enemmän tietoa ja samalla tietoturvauhkien uhkakuvat vakavoituvat. Varsinkin teollisuudessa Esineiden Internetin laitteet ja järjestelmät keräävät ja prosessoivat paljon erittäin yksityistä dataa, mikä tekee niistä otollisia tietoturvahyökkäysten kohteita. Asian tärkeyttä painottaa myös se, että tietoturvauhkien aiheuttamat vahingot eivät välttämättä kohdistu pelkästään dataan, vaan myös fyysiseen omaisuuteen tai jopa ihmishenkiin. (Sadeghi, Wachsmann & Waidner, 2015)

Tutkielmassa selviää, kuinka suuria järjestelmä- ja laitteistokokonaisuuksia teollinen Esineiden Internet käsittää. Järjestelmät keräävät ja prosessoivat valtavia määriä yksityistä dataa, mikä tekee niistä houkuttelevia hyökkäyksen kohteita (Sadeghi ym. 2015). Tietoturvauhkien muotoja on paljon erilaisia, sillä teollisen Esineiden Internetin järjestelmät ovat niin suuria, että niistä löytyy monta eri hyökkäysrajapintaa. Laitteiden tietotekniset resurssit ovat usein niin pienet, että vahvojen tietoturvamekanismien implementoiminen on todella haasteellista, mikä taas lisää tietoturvauhkien määrää. Myös standardisoinnin puute vaikuttaa niin laitteistoon kuin ohjelmistoihin ja aiheuttaa tietoturva-aukkojen myötä myös tietoturvauhkia.

Tietoturvauhkien ratkaisut ovat vielä suurelta osin tutkimuksen kohteena ja olemassa olevia ratkaisuja ei ole vielä montaa, mutta tutkielmassa esitellään joitain valmiita ratkaisuja. ARM TrustZone ja turvallisuusohjain ovat laitteistopohjaisia ratkaisuita, jotka parantavat laitteiston tietoturvaa. Käyttäjien koulutus on myös paljon painotettu ratkaisu tietoturvan parantamiseksi, sillä käyttäjän sanotaan usein olevan järjestelmän heikoin lenkki (Krombholz, Hobel, Huber & Weippl, 2015).

2 ESINEIDEN INTERNET - RAKENNE JA TEKNOLOGIAT

Tässä luvussa esitellään Esineiden Internetin perusteita ja käsitellään sen rakenne sekä yleisimmät teknologiat.

2.1 Rakenteen kuvaus

Hieman tarkentavan määritelmän Esineiden Internetistä esittää Sicari ym. 2015, joiden mukaan loogisesta perspektiivistä katsottuna Esineiden Internet koostuu älylaitteista, jotka kommunikoivat ja jakavat tietoa keskenään yhteisen tavoitteen saavuttamiseksi. Teknologisesta perspektiivistä katsottuna taas Esineiden Internetin eri osat voivat käyttää erilaisia prosessointiin ja kommunikointiin liittyviä arkkitehtuureja, teknologioita ja suunnittelumetodeja perustuen niiden tavoitteisiin (Sicari ym. 2015). Molemmista määritelmistä voi todeta, että Esineiden Internet muodostuu heterogeenisestä joukosta laitteita ja sensoreita. Rakenteen heterogeenisyys aiheuttaa haasteita arkkitehtuurin määrittelyssä ja määrittelytapoja on eriäviä. Esittelen tutkielmassani yleisesti käytetyn ja monen muun arkkitehtuurimääritelmän pohjana olevan kolmiosaisen jaon. Zhu ym. (2010) esittävät tämän kolmiosaisen jaon seuraavasti:

- **Havainnointikerros** pyrkii keräämään ja prosessoimaan dataa fyysisestä maailmasta. Tämä koostuu kahdesta osasta: sensorilaitteista ja langattomista sensoriverkoista (WSN). Sensorilaitteilla käsitetään esimerkiksi RFID-laitteet, kamerat ja turvalaitteet. Langaton sensoriverkko on automaattisesti itseään organisoiva langaton verkko, joka koostuu useista sensorisolmuista. Sensorilaitteet mittaavat koordinoidusti fyysisen ympäristön tilaa. Tarkennettuna havainnointikerros kerää ensin tiedonkeruulaitteella dataa, jonka jälkeen data siirretään seuraavalle kerrokselle käyttäen RFID:tä, Bluetoothia tai jotain muuta teknologiaa. Havainnointikerros on, ennen kaikkea, perusta Esineiden Internetin järjestelmälle. (Zhu ym. 2010, 348-349)
- **Kuljetus- tai verkkokerros** pyrkii siirtämään dataa pidempiä matkoja käyttäen erilaisia verkkoteknologioita kuten mobiilidataverkkoa, Wi-Fi:ä ja muita tiedonsiirtoteknologioita. Näin havainnointikerroksella kerättyä dataa voidaan siirtää etänä. PItkän matkan langalliset sekä langattomat verkkoteknologiat ja verkkotekniikat ovat oleellisia tämän kerroksen toiminnan kannalta. (Zhu ym. 2010, 349)
- **Käyttökerroksen** pääasiallisina tarkoituksina on datan prosessointi ja palveluiden tarjoaminen. Kuljetuskerrokselta saatu data annetaan

käytettäväksi erilaisille järjestelmille ja tietoa jalostetaan ja välitetään näin monille eri käyttäjille. (Zhu ym. 2010, 349)

2.2 Teknologiat

2.2.1 Radio Frequency IDentification

RFID eli radiotaajuinen etätunnistus (Radio Frequency IDentification system) on radioaaltoja hyödyntävä automaattinen teknologia, jonka avulla tietokoneet ja laitteet pystyvät tunnistamaan objekteja tai tallentamaan metadataa. RFID laite voi olla tagi/tarra tai lukija. Tagit ovat pieniä useasti tarraa muistuttavia laitteita, joihin on liitetty mikrosiru. Tageja kiinnitetään objekteihin, jotta nämä objektit voidaan laskea ja tunnistaa. Tagit voivat olla joko aktiivisia tai passiivisia. Aktiivisilla tageilla on oma pieni akku, joka mahdollistaa niiden kommunikoida muiden tagien kanssa. Passiiviset tagit taas saavat tarvittavan virtansa lukijalta. RFID lukijan tehtävä on aktivoida ja lukea tageja ja muodostaa niiden kanssa kommunikointiketjuja. Oleellisimpana tehtävänä lukija välittää dataa tagien ja tietojärjestelmän välillä. Dataa keräävä ja prosessoiva tietojärjestelmä on myös kattava osa RFID järjestelmää. (Jia, Feng, Fan & Lei, 2012)

RFID -järjestelmä tarjoaa nopean, joustavan ja luotettavan tavan tunnistaa, jäljittää ja hallita objekteja elektronisesti ja sitä hyödynnetään paljon erilaisissa Esineiden Internetin käyttötarkoituksissa. Esimerkiksi teollisuus ja logistiikka ovat hyödyntäneet paljon RFID:tä. Teollisuudessa varaston ylläpito ja tuotantoketjun hallinta hyödyntävät usein RFID:tä. Logistiikalle kenties oleellisin käyttöfunktio on aktiiviset tagit merikonteissa rahdin valvomiseen. (Jia ym. 2012 & Gubbi ym. 2013)

2.2.2 Near Field Communication

Toinen IoT:n havainnointikerroksessa yleisesti käytetty teknologia on **NFC** eli Near Field Communication. Siinä yhdistyy RFID:n etätunnistusteknologia sekä muita yhteysteknologioita. NFC eroaa RFID:stä kuitenkin kahdella oleellisella tavalla. NFC käyttää tunnistamiseen magneettista induktiota radiotaajuuden sijaan, joka rajoittaa etäisyyden muutamaan senttimetriin. Sitä vastoin NFC-laitteet voivat emuloida RFID tagia tai olla lukijoita ja jakaa dataa kahden virtalähteen omaavan laitteen kesken. (Nagashree, Rao & Aswini, 2014)

2.2.3 Sensoriverkot

Langattomat sensoriverkot eli WSN:t (Wireless Sensor Network) ovat Esineiden Internetin havainnointikerroksen oleellinen osa. Ne koostuvat

suuresta määrästä sensoreita, jotka ovat liitettyinä sensorisolmuihin. Solmut ovat laitteita, joihin on itegroitu mikroprosessori, muistia, virtalähde, radiotaajuuslähetin ja aktuaattori. Näiden lisäksi solmuissa on aina yksi tai useampi sensori. Sensorit voivat olla esimerkiksi magneettisia, optisia tai mekaanisia, mutta niitä kaikkia yhdistää kyky havainnoida jotain ja välittää siitä dataa. Solmun mikroprosesori käsittelee dataa ja radiotaajuuslähetintä käytetään usein datan siirtämiseen langattomasti esimerkiksi älypuhelimeen tai tietokantaan. (Yick, Mukherjee & Ghosal, 2008)

Khan ym. (2016) mainitsevat tutkielmassaan langattomiin sensoriverkkoihin liittyvän oleellisen ongelman. Verkot ovat toimiala spesifejä ja tiettyyn tehtävään orientoituja, joka tekee niiden jälkikäteen kustomoinnista tai uudelleenkäytöstä todella haastavaa ja aikaa vievää. Esineiden Internetin ja standardisaation myötä tulevaisuuden sensoriverkot tulevat hyvin mahdollisesti olemaan yhteensopivampia ja pitkäikäisempiä. (Khan ym. 2016) Gaj, Jasperneite ja Felser (2013) toteavatkin tutkimuksessaan, että standardisointi ja yhteensopivuus ovat avaintekijöitä teollisen kommunikaation kannalta.

Atzori, Iera ja Morabito (2010) esittävät tutkimuksessaan, että NFC, WSN ja RFID -teknologiat tulevat linkittämään todellisen maailman digitaaliseen maailmaan. Näin on jo tähän päivään mennessä käynytkin, sillä näitä teknologioita voi havaita ympäristössämme. Ostokset voi maksaa helposti älypuhelimen NFC:n tai lähimaksulla varustetun maksukortin RFID:n avulla käyttämällä puhelinta tai maksukorttia maksupäätteen vierellä. Väite pitää varmasti vieläkin paikkansa, sillä näiden teknologioiden käyttö tulee luultavimmin kasvamaan ja yleistymään vielä monessa muussakin käyttötarkoituksessa.

2.3 Sovelluksia ja ominaisuuksia

Esineiden Internet on saanut jo monia käytännön sovelluksia monilla eri aloilla sekä kuluttajille että yrityksille. Vaikka sovelluksia on paljon erilaisia, ryhmittelevät Atzori ym. (2010) tutkielmassaan yleisimmät näistä: kuljetustoimi, terveydenhuolto, äly-ympäristöt sekä henkilökohtainen ja sosiaalinen puoli. Chen ym. (2014) lisäävät tähän luokitteluun myös teollisuuden, joka on suuri toimiala Esineiden Internetin piirissä. Kuluttajille läheisin Esineiden Internetin sovellus on varmasti kotiautomaatio, josta esimerkkinä voidaan pitää Google Home tai Amazon Echo järjestelmää. Niissä koti varustetaan yhdellä tai useammalla verkkoon kytketyllä älykaiuttimella, joiden kanssa käyttäjä voi kommunikoida.

Chenin ym. (2014) mukaan kaikki Esineiden Internetin sovellukset sisältävät joitain näistä ominaisuuksista:

- **Paikkatiedon tunnistus ja tiedon jakaminen.** Päätesolmut keräävät paikkatietoja, käsittelevät niitä ja tarjoavat palveluja niiden perusteella.

Paikkatieto voidaan kerätä hyödyntämällä esimerkiksi maailmanlaajuista paikallistamisjärjestelmää (GPS), RFID:tä tai matkapuhelimen ID:tä. Paikkatiedon hyödyntämisellä voidaan muun muassa hallita liikenneruuhkia ja toteuttaa liikennetietojärjestelmiä.

- **Ympäristön aistiminen.** Esineiden Internetin järjestelmät pystyvät sensorisolmujen välityksellä keräämään ympäristöstä aistittua tietoa. Sensorit aistivat yleensä joko lämpöä, ilmankosteutta, melua, näkyvyyttä, valoa, säteilyä, saasteita, kuvia tai kehonliikkeitä. Ympäristöä aistivat sovellukset voivat tunnistaa muutoksia ympäristössä ja ennustaa esimerkiksi luonnon katastrofeja. Ympäristön aistimista voidaan hyödyntää myös terveydenhuollon sovelluksissa, jotka aistivat ja mittaavat potilaasta tietoa.
- **Etäohjaus.** Esineiden Internetin järjestelmillä pystytään etäohjaamaan IoT-terminaaleja, jotka voivat olla pitkänkin matkan päässä. Etäohjaus sallii Esineiden Internetin järjestelmien kokonaisvaltaisen hallinnan, jonka takia esimerkiksi onnettomuustilanteessa häviöitä ja tuhoja voidaan usein minimoida.
- **Ad Hoc verkostoitumisen** oletetaan muodostavan Esineiden Internetin järjestelmille nopeasti itseorganisoituvia verkostoitumiskykyjä, jonka avulla voidaan tuottaa lisää palveluja. Älyautojen välillä liikkuva ja organisoituva data ja siitä koituva ruuhkaton liikenne on yksi visio Ad Hoc verkostoitumisesta.
- **Turvallinen tiedonsiirto.** Esineiden Internetin järjestelmien tulee pystyä siirtämään tietoa turvallisesti sovelluksen tai palvelualustan ja IoT-terminaalien välillä.

		Sijainnin paikannus ja jakaminen	Ympäristön aistiminen	Etäohjaus	Ad Hoc verkostoi-tuminen	Turvallinen tiedonsiirto
E-terveys	Valvonta	√	√		√	√
	Kotihoito	√	√			√
ITS (Älyliikenne)	Smart fleet	√	√			√
	Auto	√	√	√	√	√
Älykaupunki	Ympäristön valvonta	√	√			√
	Turvallisuus	√	√			√
	Ruoan jäljittäminen	√				√
	Älymaatalous		√	√		√
Teollisuus	Prosessin valvonta		√	√		√
	Logistiikan hallinta	√				√

KUVIO 1 Esineiden Internetin sovelluksia & ominaisuuksia (Chen ym. 2014, s. 351)

Kuviossa 1 voidaan nähdä, millaisia ominaisuuksia tietyissä Esineiden Internetin sovelluksissa täytyy olla. Kaikki edellä mainitut ominaisuudet eivät tietenkään ole tarpeellisia kaikille Esineiden Internetin sovelluksille, vaan niihin on implementoitu vain niiden käyttötarkoitukselle oleellisia ominaisuuksia. Kuviosta voimme erottaa kuitenkin yhden ominaisuus ylitse muiden: turvallinen tiedonsiirto. Sen tärkeyttä ei voi väheksyä millään Esineiden Internetin osa-alueella ja sen oleellisuus on motivoinut myös tämän tutkielman tekemiseen. Tietoturvan oleellisuutta painottavat myös Abomhara ja Køien (2015) tutkielmassaan ja lisäävät, että datan turvallinen kerääminen ja säilöminen Esineiden Internetin sovelluksissa ovat vielä asioita, jotka vaativat paljon lisää tutkimusta ja kehitystä.

2.4 Esineiden Internet teollisuudessa

Sadeghi ym. (2015) kertovat tutkielmassaan, että teollisen Esineiden Internetin trendinä on lähivuosina ollut yhdistää tehtaiden eri osastojen itsenäisiä tuotannonohjausjärjestelmiä liittämällä niitä yhteen, lisäämällä monipuolisempia komponentteja ja integroida näitä järjestelmiä tavanomaisiin yritysjärjestelmiin. Tämä integraatio johtaa huomattavasti joustavampaan ja resursseja säästävämpään tuotantoon ja tätä myöten parempaan kustannustehokkuuteen, vaikkakin tuo mukanaan myös monia haasteita (Sadeghi ym. 2015).

Keskeinen käsite teollisessa Esineiden Internetissä on kyberfyysiset järjestelmät eli CPS (Cyberphysical System). Kumar ja Patel (2014) määrittelevät tutkielmassaan ytimekkäästi, että kyberfyysiset järjestelmät ovat järjestelmiä, jotka valvovat ja ohjaavat fyysisiä prosesseja. Baheti ja Gill (2011) täydentävät näkemystä hieman ja määrittelevät kyberfyysiset järjestelmät uuden aikakauden järjestelmiksi, joihin on integroitu tietoteknisiä ja fyysisiä kykyjä ja jotka pystyvät olla vuorovaikutuksessa ihmisten kanssa monin eri tavoin. Sadeghi ym. (2015) kertovat tutkimuksessaan nykypäivän älytehtaista, jotka ovat tehtaita, joissa kyberfyysiset järjestelmät organisoivat ja optimoivat tuotantoprosessia sekä resursseja perustuen dataan, jota kyberfyysinen järjestelmä kerää ja analysoi. Aiemmin mainittiin trendi siitä, että nykypäivänä yhdistetään tehtaiden eri osastojen itsenäisiä tuotannonohjausjärjestelmiä, lisätään monipuolisempia komponentteja ja integroidaan näitä järjestelmiä yritysjärjestelmiin. Tämän prosessin Lopputuloksena on kyberfyysinen tuotannonohjausjärjestelmä eli CPPS (Cyberphysical Production System) (Sadeghi ym. 2015).

3 TIETOTURVAUHKAT, HAASTEET JA RATKAISUT

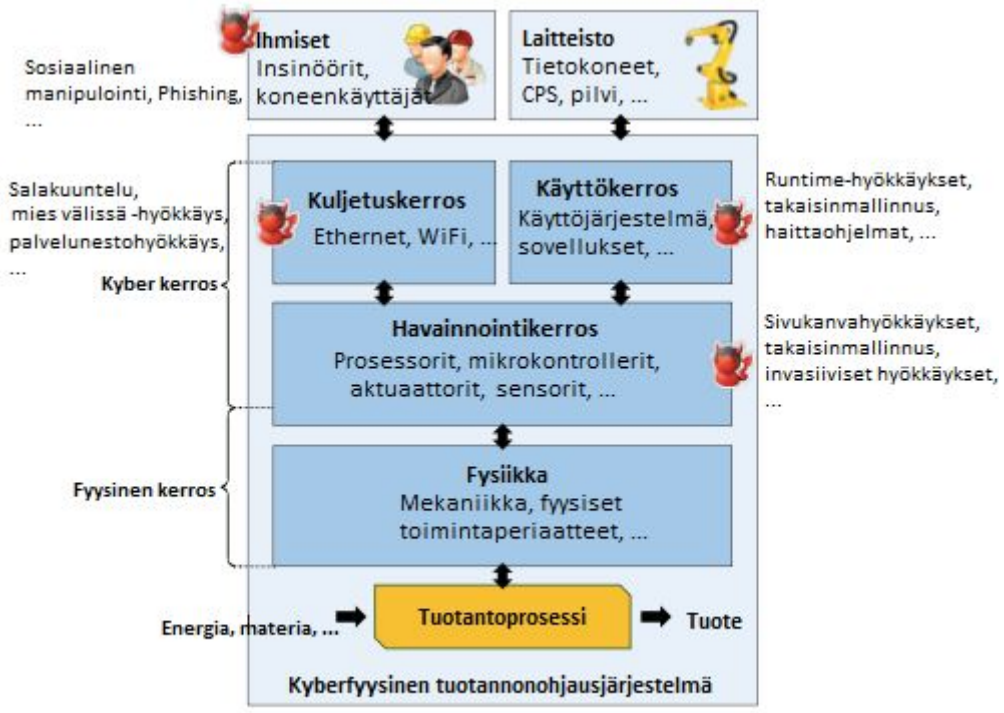
Vaikka Esineiden Internetin sovellukset ovat muuttaneet maailmaa monella tapaa niin kuluttajien keskuudessa kuin teollisuudessakin, on muutoksella ja sen tuomilla hyödyillä kääntöpuolensa. Maailman digitalisoituessa kyberturvallisuuden asema on kasvanut jatkuvasti ja Esineiden Internetin yleistyessä sen asema tulee kasvamaan ennestään. Sadeghi ym. (2015) toteavat tutkimuksessaan, että teollisuuden yrityksissä Esineiden Internetin sovellukset tuottavat ja prosessoivat suuria määriä erittäin yksityistä dataa, mikä tekee niistä otollisia kyberhyökkäyksen kohteita. He mainitsevat myös, että kyberhyökkäykset suuriin Esineiden Internetin järjestelmiin ovat erittäin vakavia, sillä ne voivat aiheuttaa fyysistä vahinkoa tai jopa uhata ihmishenkiä. He lisäävät, että näiden järjestelmien monimutkaisuus ja kyberhyökkäysten vaikutukset tuovat mukanaan uusia uhkakuvia (Sadeghi ym. 2015). Tietoturvan merkitystä teollisessa Esineiden Internetissä korostaa myös se, että teollisten toiminnanohjausjärjestelmien kohdalla turvallisuudesta puhuttaessa sillä tarkoitetaan niin tietoturvaa kuin siitä johtuvaa ihmisten ja ympäristön turvaa (Zhao & Ge, 2013).

Teollisuudessa käytetään nykypäivänä miljoonia erilaisia Esineiden Internetin laitteita erilaisiin käyttötarkoituksiin ja laitteiden määrä kasvaa jatkuvasti. Niitä käytetään ohjaus- sekä tuotantojärjestelmissä ja komponentit kommunikoivat keskenään suljetussa verkossa. Näihin sulautettuihin järjestelmiin ja niiden laitteisiin liittyy useita tietoturvariskejä ja -puutteita. Vaikka tehtaiden verkot, jossa Esineiden Internetin komponentit kommunikoivat, ovat usein suljettuja, on ne kuitenkin useasti kytketty myös internetiin. Tämä seikka on mielestäni kriittisimpiä kohtia tietoturvan kannalta, silti vaikka välissä olisi hyväkin palomuuri, on tietomurron riski silti aina olemassa, kun laitteet on yhteydessä internetiin. Sen lisäksi Costin ym. (2014) toteavat tutkimuksessaan, että sulautettujen järjestelmien ohjelmistoissa on lukuisia tietoturva-aukkoja ja haavoittuvuuksia. Pipkin (2000) ja Bertino, Martino, Paci ja Squicciarini (2010) määrittelevät haavoittuvuudet heikkouksiksi järjestelmissä tai niiden suunnittelussa, jotka sallivat hyökkääjille pääsyn luvattomaan dataan, mahdollistavat hyökkääjän suorittaa palvelunestohyökkäyksiä tai sallivat hyökkääjän suorittaa järjestelmässä komentoja.

3.1 Tietoturvauhkien muodot

Teollinen Esineiden Internet koostuu monesta eri kerroksesta ja suuresta määrästä laitteita, ohjelmistoja ja rajapintoja. Havainnointi-, kuljetus- ja käyttökerroksen lisäksi myös järjestelmien ja laitteiden käyttäjät ovat yksi hyökkäysrajapinta. Sadeghi ym. (2015) esittävät tutkielmassaan

havainnollistavan kuvion kyberfyysisen tuotannonohjausjärjestelmän rakenteesta ja sen hyökkäysrajapinnoista.



KUVIO 2 Kyberfyysisen tuotannonohjausjärjestelmän arkkitehtuuri ja hyökkäysrajapinnat. Muokattu. (Sadeghi ym. 2015)

Kuviosta 2 voidaan nähdä, kuinka monesta eri osa-alueesta teollinen kyberfyysinen tuotannonohjausjärjestelmä muodostuu. Usea eri osa-alue ja rajapinta johtaa myös siihen, että tietoturvaa heikentäviä hyökkäysrajapintoja ja hyökkäysmuotoja on useita erilaisia. Seuraavaksi käydään läpi rajapintojen yleisimmät hyökkäysmuodot.

3.1.1 Havainnointikerros

Havainnointikerroksen pienet laitteet, sensorit ja komponentit ovat haavoittuvaisia useille eri hyökkäyksille. Yksi yleisistä hyökkäysten muodoista on **sivukanavahyökkäykset**. Babar ym. (2011) määrittelevät tutkimuksessaan sivukanavahyökkäykset kryptografisiksi hyökkäyksiksi, jotka perustuvat sivukanavainformaatioon, jota kryptografiaa hyödyntävät laitteet lähettävät. He lisäävät, että tällaista informaatiota ovat esimerkiksi ajoitustieto, virrankulutus, elektromagneettiset päästöt ja ääni. He kertovat, että näitä tietoja hyväksi

käyttämällä voi hyökkääjä vaurioittaa laitteita ja järjestelmiä. Cherednichenko, Baranov ja Morozova (2013) lisäävät, että monet sivukanavahyökkäykset vaativat teknistä tietämystä järjestelmän ja laitteiston sisäisestä toiminnasta. **Invasiiviset hyökkäykset** ovat hyökkäyksiä, jossa hyökkääjä pääsee fyysisesti kontaktiin laitteiden kanssa ja pystyy näin joko saamaan salattuja tietoja, vahingoittamaan laitteita tai häiritsemään niiden toimintaa sekä tiedonsiirtoa. Fernández-Caramés, Fraga-Lamas, Suárez-Albela ja Castedo (2016) esittävät tutkielmassaan, että RFID tagiin voi kohdistaa fyysistä signaalin jumittamista, tagin voi irrottaa tai sen voi tuhota erinäisin keinoin. He lisäävät, että RFID tagin pystyy myös takaisinmallintamaan. **Reverse engineering eli takaisinmallinnus** on hyökkäysmenetelmä, jota pystytään hyödyntämään sekä kuljetus- että käyttökerroksessa. Takaisinmallinnuksessa ohjelmistoa tai laitteistoa lähdetään purkamaan ja analysoimaan hienostuneesti niin, että saadaan aikaan uudelleenmallinnus tuotteesta. Tämä prosessi tuottaa paljon informaatiota tuotteen toiminnasta sekä suunnittelusta ja hyökkääjien agendana on useasti löytää tietoturva-aukkoja ja haavoittuvuuksia tai emuloida laite tai ohjelmisto. Osa sivukanavahyökkäyksistä voivat vaatia takaisinmallinnusta. Fernández-Caramés ym. (2016) mainitsevat esimerkkinä kommunikaatioprotokollahyökkäyksen, joka on takaisinmallinnusta vaativa sivukanavahyökkäys. He kertovat, että hyökkäyksessä kahden laitteen välinen kommunikaatio tallennetaan, analysoidaan ja käytetään laitteiden uudelleenmallinnukseen.

3.1.2 Kuljetuskerros

Kuljetuskerroksessa datan kuljettamiseen käytettävät useat teknologiat ja protokollat mahdollistavat myös useita hyökkäysmuotoja. **Salakuunteluhyökkäys** eli eavesdropping on kuljetuskerroksessa tapahtuva hyökkäys, jossa hyökkääjä varastaa dataa kahden verkossa kommunikoivan laitteen väliltä. Esineiden Internetin laitteet tuottavat, välittävät ja analysoivat suuria määriä dataa, mikä tekee mielestäni salakuunteluhyökkäyksistä erityisen vakavia Esineiden Internetin kannalta. **Mies välissä -hyökkäys** eli Man-in-the-Middle tunnetaan suomeksi myös nimellä välistävetohyökkäys, joka kuvaa sen luonnetta hyvin. Conti, Dragoni ja Lesyk (2016) kertovat tutkimuksessaan, että Mies välissä -hyökkäyksessä on yleensä osallisena kaksi päätelaitetta eli uhria ja kolmas osapuoli eli hyökkääjä. He lisäävät, että hyökkääjällä on pääsy uhrien päätelaitteiden väliselle kommunikaatiokanavalle ja pystyy manipuloimaan tietoa välissä (Conti ym. 2016). Carl, Kesidis, Brooks ja Rai (2006) esittävät, että **palvelunestohyökkäys** eli Denial of Service on hyökkäysmuoto, jossa hyökkääjä pyrkii kaatamaan laitteen tai verkon kohdistamalla siihen niin paljon liikennettä, että siitä tulee käyttökelvoton. He

lisäävät, että **hajautettu palvelunestohyökkäys** eli Distributed Denial of Service on vastaava hyökkäys, mutta siinä hyökkääjällä on käytössään useita kaapattuja päätteitä, joilta hän voi kohdistaa liikennettä hyökättävään kohteeseen (Carl ym. 2006).

3.1.3 Käyttökerros

Käyttökerroksen dataa prosessoivat ja palveluita tarjoavat sovellukset toimivat myös erilaisten hyökkäysten rajapintoina. **Runtime-hyökkäys** eli ajonaikainen tiedonkeräyshyökkäys viittaa hyökkäysmalliin, jossa hyökkääjä pyrkii keräämään sovelluksen tuottamaa tai vastaanottamaa dataa sovelluksen ajon aikana (Zhang ym. 2015). **Haittaohjelmaksi** kutsutaan ohjelmistoa, jonka tarkoituksena on päästä salaa uhrin laitteelle ja aiheuttaa vahinkoa tai vakoilla dataa. Haittaohjelmia on montaa eri tyyppiä kuten virus, troijalainen, mato, spyware tai ransomware. Poulsen (2003) kertoo raportissaan Slammer madosta, joka saastutti Ohion ydinvoimalan verkon ja kaatoi valvontajärjestelmän moneksi tunniksi. Edellä mainittu takaisinmallinnus on uhkana myös sovellusten tapauksessa, sillä hyökkääjät pystyy takaisinmallintamaan myös sovelluksia ja paikantamaan niistä haavoittuvuuksia.

3.1.4 Ihmiset

Kaikki haavoittuvuudet eivät liity kuitenkaan pelkästään laitteistoon, verkkoon ja sovelluksiin, vaan myös niitä käyttävät ja kehittävät ihmiset on riskitekijä. Krombholz ym. (2015) määrittelevät **sosiaalisen manipuloinnin** hyökkäykseksi, jossa hyökkääjä manipuloi ihmistä antamaan tietoa itselleen. He lisäävät, että sosiaalinen manipulointi on muihin hyökkäysmalleihin verrattuna ylivoimainen, koska sillä pystytään läpäisemään jopa huipputurvalliset järjestelmät ja verkot, sillä käyttäjät itse ovat usein järjestelmän heikoin lenkki (Krombholz ym. 2015). Myös aiemmin mainitut haittaohjelmat voivat päästä huipputurvallisten järjestelmien sisään käyttäjien kautta. Sosiaalisen manipuloinnin yksi yleisimmin käytetyistä keinoista on **phishing** eli verkkourkinta**.** Siinä hyökkääjä käyttää yleensä sähköpostia tai tekstiviestejä avukseen ja esittää mahdollisimman virallisesti ja uskottavasti jotain muuta tahoa, jonka avulla saa urkittua tietoa uhreilta. Vishing hyökkäyksessä idea on täysin sama, mutta se toteutetaan puhelimitse.

3.2 Haasteet

Sadeghi ym. (2015) toteavat tutkimuksessaan, että IT-komponenttien integroiminen teollisiin toiminnanohjausjärjestelmiin on yleensä luonut tietoturva-aukkoja ja haavoittuvuuksia. He lisäävät, että näiden haavoittuvuuksien ja tietoturva-aukkojen korjaukset tulevat yleensä viiveellä, mikä tekee nykyisistä teollisista toiminnanohjausjärjestelmistä haavoittuvaisia lukuisille kyberhyökkäyksille (Sadeghi ym. 2015). Teollisen Esineiden Internetin tietoturvan parantamiseen luo oman vaikeuden myös se, että Esineiden Internetin laitteisiin on vaikea implementoida vahvoja tietoturvamekanismeja, sillä ne ovat yleensä pieniä ja täten niiden laskentateho, muistin määrä ja akun kapasiteetti ovat rajallisia (Køien, 2011).

Järjestelmien tietoturva-aukkoja ja haavoittuvuuksia voi esiintyä järjestelmän laitteistossa tai ohjelmistossa, heikoissa toimintatavoissa järjestelmän käytössä tai heikoissa käyttäjissä (Kizza, 2013). Laitteiston ja ohjelmiston tapauksessa Abomhara ja Køien (2015) toteavat tutkimuksessaan, että Esineiden Internet perustuu näihin kahteen kokonaisuuteen ja niistä löytyy useasti suunnitteluvirheitä. He jatkavat, että laitteiston suunnitteluvirheitä on usein erittäin vaikea todeta ja diagnosoida ja myöskin erittäin vaikeita korjata. He lisäävät, että ohjelmiston haavoittuvuuksia ja tietoturva-aukkoja esiintyy käyttöjärjestelmissä, ohjelmissa ja laiteohjaimissa ja että nämä haavoittuvuudet johtuvat yleensä muun muassa huonosta projektinjohdosta, huonosta kommunikaatiosta suunnittelijoiden ja käyttäjien välillä sekä resurssien ja taitojen puutteesta (Abomhara & Køien, 2015).

Kryptografialla suojattu tietoliikenne salaa monia muita yhteyksiä maailmanlaajuisesti, mutta Esineiden Internetin kohdalla sen implementoiminen on haastavaa. Kuten Køien (2011) aiemmin mainitsi laitteiden pienistä resursseista, K Xu, Ren, Song ja Du (2016) ovat tutkielmassaan samaa mieltä ja lisäävät, että Esineiden Internetin laitteiden resurssien ollessa yleensä kovin pienet kryptografian implementoiminen niihin on erittäin hankalaa, sillä se vaatii laitteilta lisää resursseja ja laskentatehoa. He mainitsevat myös, että hyökkääjien laskentatehon lisääntyessä jopa kryptografiset suojausmetodit voivat vuotaa informaatiota, jonka vuoksi Esineiden Internetin salatun tietoliikenteen takaamiseksi on kehitettävä uusia tehokkaita tiedonsuojausprotokollia. Wurm ym. (2016) lisäävät aiheeseen, että tulevaisuudessa tulee olemaan vakavia tietoturvaongelmia, jos tämänhetkistä Esineiden Internetin laitteiden suunnittelutyyliä jatketaan.

Standardoinnin puute ja verkkojen laitteiden heterogeenisyys ovat myös suuria haasteita teollisessa Esineiden Internetissä. Mahmoud, Yousuf, Aloul ja Zualkernan (2015) mainitsevat tutkielmassaan, että laitteiden heterogeenisyys tekee vallitsevien verkkoprotokollien käytön haasteelliseksi niin, että tietoturvan taso säilyisi korkeana. He kertovat myös, että standardoinnin puute Esineiden Internetin sovelluksissa aiheuttaa sovellusten tietoturvattomuutta.

He lisäävät, että eri sovellukset käyttävät eri todentamismekanismeja, mikä tekee niiden tietoturvallisesta integroimisesta todella haastavaa.

3.3 Ratkaisut

Vaikka Esineiden Internetin tietoturvaongelmien ratkaisujen puhutaan useissa tutkimuksissa olevan vielä tulevaisuuden tutkimuksen tulos, on joitain ratkaisuja ongelmien ratkaisemiseksi jo esitetty.

Lesjak, Hein ja Winter (2015) esittävät tutkielmassaan kaksi laitteistotasoista ratkaisua teolliseen Esineiden Internetiin: ARM TrustZone ja turvallisuusohjain. ARM TrustZone pyrkii turvaamaan Esineiden Internetin laitteet jakamalla niiden komponentit kahteen loogiseen osioon, punaiseen ja vihreään, jotka kommunikoivat toistensa kanssa. GlobalPlatform on luonut jo erän julkisia standardeja ARM TrustZone alustoille, mikä tekee siitä mielenkiintoisen alustan tulevaisuuden teollisen Esineiden Internetin kannalta. Turvallisuusohjain sitä vastoin on fyysinen mikrokontrolleri, joka sisältää sarjan kryptografisia operaatioita. Turvallisuusohjain pystyy suojaamaan tehokkaasti sekä verkon yli tapahtuvilta hyökkäyksiltä että invaasivisilta hyökkäyksiltä, sillä kaikki kryptografiset avaimet on säilötty sen sisään. Turvallisuusohjaimen hyvänä puolena onkin erittäin korkea tietosuoja, mutta ARM TrustZone on joustavampi ja tehokkaampi. Tutkimuksessa todetaankin, että näiden kahden teknologian yhdistelmä tarjoaisi maksimaalisen tietoturvan teollisen Esineiden Internetin tarpeisiin. (Lesjak ym. 2015)

Käyttäjien tietoisuutta ja tietoturvakoulutusta ei voi mielestäni painottaa liikaa. Tätä väitettä tukee Pattonin ym. (2014) tutkimus käyttäjien heikoista tietoturvakäytänteistä Esineiden Internetin laitteissa. Tutkimus osoitti, että moniin laitteisiin on jätetty oletussalasanat tai salasanoja ei ollut ollenkaan. He ilmaisevat tutkimuksessa myös, että Esineiden Internetin kasvaessa nämä käytänteet tekevät Esineiden Internetistä enemmän haitallista kuin hyödyllistä ja että organisaatioiden sekä käyttäjien on aika ottaa vastuullisempi ja ennakoivampi suhtautuminen Esineiden Internetin tietoturvallisuuteen (Patton ym. 2014).

4 YHTEENVETO

Tässä tutkielmassa tutkittiin teollisen Esineiden Internetin yleisimpiä tietoturvauhkia, niihin liittyviä haasteita ja ratkaisuja. Tutkielma suoritettiin kirjallisuuskatsauksena käymällä läpi aiheeseen liittyviä tieteellisiä artikkeleita ja tutkimuksia. Todettiin, että teolliseen Esineiden Internetiin liittyy suuri määrä tietoturvauhkia ja niiden ratkaisemiseen liittyy useita haasteita. Haasteisiin on olemassa joitain ratkaisuja, mutta suuri osa ratkaisuista on vielä kehityksen tai tutkimuksen alla. Tämä aiheutti haasteen tutkielman viimeisen osion kannalta, sillä tutkielmassa esitettiin pelkästään olemassa olevia ratkaisuja. Tulevaisuuden kannalta teollisen Esineiden Internetin tietoturvallisuuden tilanne näyttää kuitenkin paremmalta, sillä tutkimusta ja kehitystä tietoturvan parantamiseksi tehdään paljon.

Esineiden Internet voidaan jakaa usealla tavalla eri kerroksiin. Tässä tutkielmassa esiteltiin kolmikerroksinen arkkitehtuurimalli, joka on monen muun arkkitehtuurinmääritelmän pohjana. Kolmiosaiseen arkkitehtuurimalliin kuuluu havainnointi-, verkko- ja käyttökerros. Havainnointikerroksesa sensorilaitteet keräävät ja prosessoivat dataa ja välittävät sitä sensoriverkoissa. Verkkokerroksessa erilaiset tiedonsiirtoteknologiat siirtävät havainnointikerroksessa kerättyä dataa pidempiä matkoja. Käyttökerroksessa kuljetuskerrokselta saatua dataa prosessoidaan ja tarjotaan palveluita käyttäjille.

Esineiden Internetin toiminnan kannalta kolme oleellista avainteknologiaa ovat Radio Frequency IDentification (RFID), Near Field Communication (NFC) ja Sensoriverkot (WSN). RFID on radioaaltoja hyödyntävä etätunnistusteknologia, jonka avulla laitteet pystyvät tunnistamaan objekteja ja tallentamaan dataa. RFID laitteet ovat joko tageja tai lukijoita. Tageissa on pieni mikrosiru, joka pystyy säilömään dataa. Tageja kiinnitetään objekteihin ja lukijoilla luetaan tietoja niistä. NFC:ssä yhdistyy RFID:n etätunnistusteknologia sekä muita yhteysteknologioita. Radioaaltojen sijaan se käyttää magneettista induktiota ja NFC-laitteet voivat olla joko tarroja tai lukijoita. Sensorivekot koostuvat sensoreista, jotka havainnoivat ympäristöä ja välittävät dataa havainnoistaan. Sensorit ovat yhteydessä sensorisolmuihin, jotka käsittelevät dataa ja siirtävät sitä eteenpäin.

Esineiden Internetille on kehittynyt useita sovelluksia ja ominaisuuksia. Yleisimpiä sovelluksia ovat kuljetustoimi, terveydenhuolto, äly-ympäristöt, henkilökohtainen sekä sosiaalinen puoli ja teollisuus. Näille sovelluksille on määritelty tiettyjä ominaisuuksia, joita tietyissä sovelluksissa on oltava. Näitä ominaisuuksia ovat paikkatiedon tunnistus & jakaminen, ympäristön aistiminen, etäohjaus, Ad Hoc verkostoituminen ja turvallinen tiedonsiirto. Näistä ominaisuuksista eniten vaadittu on selkeästi turvallinen tiedonsiirto.

Teollisuudessa oleelliset käsitteet Esineiden Internetin kannalta ovat kyberfyysiset järjestelmät (CPS) ja kyberfyysiset tuotannonohjausjärjestelmät (CPPS). Kyberfyysiset järjestelmät ovat järjestelmiä, joihin on itegroitu tietoteknisiä sekä fyysisiä kykyjä ja jotka valvovat ja ohjaavat fyysisiä

prosesseja. Kyberfyysiset tuotannonohjausjärjestelmät ovat hieman laajempia järjestelmäkokonaisuuksia, jotka on integroitu yritysjärjestelmiin. Tällaiset järjestelmät johtavat resursseja säästävämpään ja joustavampaan tuotantoon ja sitä myöten kustannustehokkuuteen.

Teolliseen Esineiden Internetiin liittyy kuitenkin myös tietoturvahaasteita. Teollisuuden Esineiden Internetin järjestelmät tuottavat ja prosessoivat paljon yksityistä dataa, mikä tekee niistä houkuttelevia kyberhyökkäyksen kohteita. Näiden hyökkäysten vaikutukset voivat olla vakavia, sillä ne voivat pahimmillaan aiheuttaa fyysistä vahinkoa tai uhata jopa ihmishenkiä. Nämä hyökkäykset mahdollistaa useat tietoturva-aukot ja haavoittuvuudet, joita järjestelmien kokonaisuuksista löytyy. Haavoittuus on heikkous järjestelmässä, joka mahdollistaa hyökkääjälle pääsyn luvattomaan dataan ja sallii hyökkään suorittaa järjestelmässä komentoja ja hyökkäyksiä.

Kyberfyysiset järjestelmät ja tuotannonohjausjärjestelmät ovat niin suuria kokonaisuuksia, että niissä on useita hyökkäysrajapintoja. Havainnointikerroksessa yleisimpiä hyökkäysmuotoja ovat sivukanavahyökkäykset, invasiiviset hyökkäykset ja takaisinmallinnus. Sivukanavahyökkäyksessä hyökkääjä hyväksikäyttää laitteen lähettämää sivukanavainformaatiota. Invasiivisessa hyökkäyksessä hyökkääjä pääsee fyysisesti kontaktiin laitteiden kanssa ja pystyy saamaan salattuja tietoja itselleen, tuhoamaan tietoja tai hajottamaan laitteita. Takaisinmallinnus on menetelmä, jossa hyökkääjä lähtee purkamaan ja analysoimaan laitetta ja tekee siitä uudelleenmallinnuksen. Tämän tuloksena hyökkääjä voi löytää laitteesta tietoturva-aukkoja, joita hän voi hyväksikäyttää.

Verkkokerroksen yleisimmät hyökkäysmuodot ovat salakuuntelu-, mies välissä- ja palvelunestohyökkäys. Salakuunteluhyökkäyksessä hyökkääjä varastaa dataa kahden verkon yli kommunikoivan laitteen väliltä. Mies välissä -hyökkäyksessä hyökkääjä pystyy manipuloimaan kahden päätelaitteen välistä kommunikaatiota. Palvelunestohyökkäyksessä kohdistetaan niin paljon tietoliikennettä hyökättävää verkkoa tai palvelinta kohtaan, että siitä tulee käyttökelvoton. Hajautetussa palvelunestohyökkäyksessä hyökkääjällä on hallussaan useita kaapattuja päätteitä, joilta hän voi kohdistaa tietoliikennettä hyökkäyksen kohteeseen.

Käyttökerroksen hyökkäysmallit ovat ajonaikainen hyökkäys, haittaohjelmat ja takaisinmallinnus. Ajonaikaisessa hyökkäyksessä hyökkääjä pyrkii salaa keräämään sovelluksen tuottamaa, prosessoimaa tai vastaanottamaa dataa sovelluksen ajon aikana. Haittaohjelmat ovat ohjelmia, joiden tarkoituksena on päästä salaa uhrin koneelle ja aiheuttaa vahinkoa tai vakoilla dataa. Takaisinmallinnus toimii käyttökerroksessa samalla periaatteella kuin havainnointikerroksessakin, mutta kohteena on ohjelmistot.

Vaikka käyttäjät eivät kuulu esitellyn kolmiosaiseen arkkitehtuurimalliin, sanotaan heidän olevan järjestelmän heikoin lenkki. Käyttäjiin voidaan kohdistaa sosiaalista manipulaatiota, joka on myös yksi hyökkäysmalli. Sosiaalisessa manipulaatiossa hyökkääjä esittää olevansa joku muu ja pyrkii manipuloimalla saamaan tietoa itselleen. Yleinen sosiaalisen

manipulaation muoto on phishing, jossa hyökkääjä käyttää yleensä sähköpostia tai tekstiviestejä avukseen käyttäjien manipuloinnissa.

Tietoturvallisen teollisen Esineiden Internetin edessä on monia haasteita. Laitteet ovat usein fyysiseltä kooltaan ja sitä myöten myös tietoteknisiltä resursseiltaan kovin pieniä. Tämä tekee vahvojen tietoturvamekanismien implementoimisesta niihin erittäin haasteellista. Hyökkääjien laskentateho myös kasvaa jatkuvasti, joka lisää haastetta edelleen uusien suojausmekanismien kehittämiseksi. Standardoinnin puute ja verkkojen laitteiden heterogeenisyys aiheuttaa myös haasteita teollisen Esineiden Internetin järjestelmissä.

Valmiita ratkaisuja haasteisiin on vähän, sillä aihe on vielä tutkimuksen ja kehityksen alla. ARM TrustZone ja turvallisuusohjain ovat laitetason tietoturvaratkaisuja, jotka suojaavat teollisen Esineiden Internetin laitteita hyökkäyksiltä. ARM TrustZone jakaa laitteen kahteen loogiseen osaan ja turvallisuusohjain on laitteeseen implementoitava mikrosiru. Oleellisena ratkaisuna voidaan pitää käyttäjien asianmukaista koulutusta, sillä käyttäjät voivat tietämättään vahingoittaa suljetuinta ja tietoturvallisintakin järjestelmää.

LÄHTEET

Abomhara, M., & Køien, G. M. (2014, May). Security and privacy in the Internet of Things: Current status and open issues. In Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on (pp. 1-8). IEEE.

Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security, 4(1), 65-88.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer networks, 54(15), 2787-2805.

Babar, S., Stango, A., Prasad, N., Sen, J., & Prasad, R. (2011, February). Proposed embedded security framework for internet of things (iot). In Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on (pp. 1-5). IEEE.'

Baheti, R., & Gill, H. (2011). Cyber-physical systems. The impact of control technology, 12(1), 161-166.

Bertino, E., Martino, L. D., Paci, F., & Squicciarini, A. C. (2009). Web services threats, vulnerabilities, and countermeasures. In Security for Web Services and Service-Oriented Architectures (pp. 25-44). Springer, Berlin, Heidelberg.

Carl, G., Kesidis, G., Brooks, R. R., & Rai, S. (2006). Denial-of-service attack-detection techniques. IEEE Internet computing, 10(1), 82-89.

Chen, S., Xu, H., Liu, D., Hu, B., & Wang, H. (2014). A vision of IoT: Applications, challenges, and opportunities with china perspective. IEEE Internet of Things journal, 1(4), 349-359.

Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man in the middle attacks. IEEE Communications Surveys & Tutorials, 18(3), 2027-2051.

Costin, A., Zaddach, J., Francillon, A., Balzarotti, D., & Antipolis, S. (2014, August). A Large-Scale Analysis of the Security of Embedded Firmwares. In USENIX Security Symposium (pp. 95-110).

Fernández-Caramés, T. M., Fraga-Lamas, P., Suárez-Albela, M., & Castedo, L. (2016). Reverse Engineering and Security Evaluation of Commercial Tags for RFID-Based IoT Applications. Sensors, 17(1), 28.

Gaj, P., Jasperneite, J., & Felser, M. (2013). Computer communication within industrial distributed environment—A survey. IEEE Transactions on Industrial Informatics, 9(1), 182-189.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 29(7), 1645-1660.

Jia, X., Feng, Q., Fan, T., & Lei, Q. (2012, April). RFID technology and its applications in Internet of Things (IoT). In Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on (pp. 1282-1285). IEEE.

Khan, I., Belqasmi, F., Glitho, R., Crespi, N., Morrow, M., & Polakos, P. (2016). Wireless sensor network virtualization: A survey. IEEE Communications Surveys & Tutorials, 18(1), 553-576.

Kizza, J. M. (2013). Guide to computer network security (pp. 387-411). London: Springer. ISO 690

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and applications, 22, 113-122.

Kumar, J. S., & Patel, D. R. (2014). A survey on internet of things: Security and privacy issues. International Journal of Computer Applications, 90(11).

Køien, G. M., & Oleshchuk, V. A. (2013). Aspects of Personal Privacy in Communications: Problems, Technology and Solutions. River Publishers.

Køien, G. M. (2011). Reflections on trust in devices: an informal survey of human trust in an internet-of-things context. Wireless Personal Communications, 61(3), 495-510.

Lesjak, C., Hein, D., & Winter, J. (2015, November). Hardware-security technologies for industrial IoT: TrustZone and security controller. In Industrial Electronics Society, IECON 2015-41st Annual Conference of the IEEE (pp. 002589-002595). IEEE.

Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015, December). Internet of things (IoT) security: Current status, challenges and prospective measures. In Internet Technology and Secured Transactions (ICITST), 2015 10th International Conference for (pp. 336-341). IEEE.

Patton, M., Gross, E., Chinn, R., Forbis, S., Walker, L., & Chen, H. (2014, September). Uninvited connections: A study of vulnerable devices on the internet of things (IoT). In Intelligence and Security Informatics Conference (JISIC), 2014 IEEE Joint (pp. 232-235). IEEE.

Pipkin, D. L. (2000). Information security: protecting the global enterprise. Prentice Hall PTR.

Sadeghi, A. R., Wachsmann, C., & Waidner, M. (2015, June). Security and privacy challenges in industrial internet of things. In Proceedings of the 52nd annual design automation conference(p. 54). ACM.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer networks, 76, 146-164.

Wurm, J., Hoang, K., Arias, O., Sadeghi, A. R., & Jin, Y. (2016, January). Security analysis on consumer and industrial iot devices. In Design Automation Conference (ASP-DAC), 2016 21st Asia and South Pacific (pp. 519-524). IEEE.

Xu, Q., Ren, P., Song, H., & Du, Q. (2016). Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations. IEEE Access, 4, 2840-2853.

Yick, J., Mukherjee, B., & Ghosal, D. (2008). Wireless sensor network survey. Computer networks, 52(12), 2292-2330.

Zhang, N., Yuan, K., Naveed, M., Zhou, X., & Wang, X. (2015, May). Leave me alone: App-level protection against runtime information gathering on android. In Security and Privacy (SP), 2015 IEEE Symposium on (pp. 915-930). IEEE.

Zhao, K., & Ge, L. (2013, December). A survey on the internet of things security. In Computational Intelligence and Security (CIS), 2013 9th International Conference on (pp. 663-667). IEEE.

Zhu, Q., Wang, R., Chen, Q., Liu, Y., & Qin, W. (2010, December). Iot gateway: Bridgingwireless sensor networks into internet of things. In Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on (pp. 347-352). Ieee.