Kodin IoT-laitteiden tietoturvan parantaminen hunajapurkkien avulla

Turun yliopisto
Tietotekniikan laitos
TkK-tutkielma
Tietotekniikka
Huhtikuu 2025
Omar Polo

TURUN YLIOPISTO
Tietotekniikan laitos

OMAR POLO: Kodin IoT-laitteiden tietoturvan parantaminen hunajapurkkien avulla

TkK-tutkielma, 36 s.
Tietotekniikka
Huhtikuu 2025

IoT-laitteiden määrän nopea kasvu ja älykotien yleistyminen ovat lisänneet merkittävästi haavoittuvien kohteiden määrää kyberrikollisten näkökulmasta. Kodin älylaitteiden, kuten valvontakameroiden, taulutelevisioiden ja älyvalojen suojaus on yleensä riittämätöntä ja voivat tarjota hyökkääjille pääsyn kotiverkkoon. Tietoturva on useille käyttäjille näkymätöntä, ja siksi tehokkaiden suojausmenetelmien kehittäminen on entistä tärkeämpää. Tässä kandidaatintutkielmassa tarkastellaan, kuinka hunajapurkkijärjestelmiä voidaan hyödyntää esineiden internetin (IoT) tietoturvauhkien havaitsemisessa ja torjumisessa.
Tässä kirjallisuuskatsauksessa perehdytän erilaisiin hunajapurkkityyppeihin, niiden teknisiin ominaisuuksiin ja siihen, miten ne voivat vahvistaa kodin älylaitteiden tietoturvaa. Lisäksi käsitellään todellisia esimerkkejä IoT-laitteisiin kohdistuneista hyökkäyksistä ja analysoidaan, mitä niistä on opittu. Hunajapurkit voivat toimia tehokkaina työkaluina hyökkäysten havaitsemisessa ja niiden avulla voidaan kerätä arvokasta tietoa erilaisista uhista, jota voidaan hyödyntää muun muassa haittaohjelmien tunnistamisessa ja puolustustoimien kehittämisessä.
Tutkielman tulokset osoittavat, että hunajapurkit soveltuvat hyvin IoT-ympäristöihin erityisesti uhkien monitorointiin ja analysointiin. Ne tarjoavat keinon havaita hyökkäyksiä jo varhaisessa vaiheessa ja tuottavat tärkeää tietoa siitä, millaisia taktiikoita hyökkääjät käyttävät. Toisaalta niiden käyttöön liittyy myös haasteita, kuten järjestelmien monimutkaisuus, ylläpitotarpeet ja mahdolliset yksityisyydensuojakysymykset. Tutkielma osoittaa, että hunajapurkit eivät ole täydellinen ratkaisu, mutta ne voivat olla arvokas osa laajempaa IoT-tietoturvastrategiaa, ja niiden hyödyntäminen tarjoaa lupaavia mahdollisuuksia tulevaisuudessa.

Asiasanat: IoT, hunajapurkit, tietoturva, kyberturvallisuus, bottiverkot, Mirai, CIA-kolmio, smart homes

Sisällys

1 Johdanto **1**

2 Tieto- ja kyberturva **4**

2.1 Kyberturva 5

2.2 CIA-kolmio 6

2.3 Tekniset toimet tietoturvan parantamiseksi 9

3 Hunajapurkit ja esineiden internet **11**

3.1 Hunajapurkit 11

3.2 Esineiden internet 17

3.3 IoT-laitteiden tietoturva ja riskit 19

3.4 Mirai-bottiverkkohyökkäys 2016 20

3.5 Motiivit, kohteet ja tekijät 21

4 Uhkien havainnointi ja ennakoiva puolustus: Hunajapurkit IoT-laitteiden turvallisuudessa **24**

4.1 Hunajapurkkien hyödyt IoT-ympäristössä 25

4.2 Hunajapurkkien havaitsemat hyökkäystekniikat 26

4.3 Hunajapurkkien haasteet ja mahdolliset tulevaisuuden kehityssuunat . . . 28

5 Yhteenveto **33**

5.1 Vastaukset tutkimuskysymyksiin 34

5.2 Jatkotutkimusaiheet 35

Lähdeluettelo **37**

1 Johdanto

Kyberturvallisuus ja tietoturvaan liittyvät riskit ovat olleet huolenaiheita niin kauan kuin tietokoneita on ollut olemassa. Tietokoneiden välityksellä tapahtuva laiton toiminta on aiheuttanut päänvaivaa 1960-luvulta asti, kun ihmiset ovat syystä tai toisesta keksineet tapoja murtautua muihin tietokoneisiin. Kybermurtovarkaan motiiveina voivat olla esimerkiksi datan varastaminen tai muuntelu taloudellisista, poliittisista tai vihamielisistä syistä. [1]. Motiivit eivät ole juurikaan muuttuneet edes 60 vuoden jälkeen, mutta hyökkäystavat ja teknologinen konteksti ovat muuttuneet dramaattisesti. Käyttäjä ei koskaan voi olla täysin varma, mitä päältä päin harmittomalta vaikuttava sähköposti tai www-linkki kätkee sisäänsä. Erityisesti viimeisen kahden vuosikymmenen aikana tietokoneiden, älylaitteiden ja internetin leviäminen on synnyttänyt kokonaan uusia rikollisuuden muotoja. Nykyään useat kyberrikokset ovat automatisoituja ja mittakaavaltaan globaaleja. Motiiveina ovat usein taloudelliset hyödyt, ilkivalta, valtiollinen vakoilu, aktivismi, maineen pilaaminen tai yritys ansaita mainetta [2]. Tämän vuoksi tietokoneista löytyy tyypillisesti esiasennettuna viruksentorjuntaohjelmia. Kyberrikollisuutta vastaan taisteleminen on jatkuva prosessi ja myös virustorjuntaohjelmia tulee päivittää säännöllisesti, sillä käyttöjärjestelmien kehittyessä myös uusia haavoittuvaisuuksia ja tapoja murtautua tietokonejärjestelmään löytyy jatkuvasti. Mutta jotta mahdollisia uhkia voidaan ennaltaehkäistä kunnolla, ohjelmistokehittäjien on saatava lisätietoa hyökkääjistä ja heidän käyttämistä metodeista. Sitten herää kysymys, että miten tällaista informaatiota saadaan kyberrikollisista irti. Koska kyberrikolliset eivät luonnollisesti paljasta toimintatapojaan vapaaehtoisesti, tämä

tieto pitää selvittää toisella tavalla, herättämällä mahdollisimman vähän huomiota. Paras keino on saada rikolliset itse näyttämään suoraan, miten he tunkeutuvat sisään laitteeseen. Tämä onnistuu johdattamalla pahaa aavistamattomat tunkeutujat varta vasten heille rakennettuun ansoitettuun ympäristöön ja napata heidät itse teossa samalla keräten tietoa heistä ja heidän toimintatavoistaan. Tällaisia valvottuja, haavoittuvaisiksi naamioituja virtuaaliansoja kutsutaan hunajapurkeiksi eli honeypoteiksi.

Tämä kandidaatintutkielma on toteutettu kirjallisuuskatsauksena. Lähteinä on käytetty pääasiassa tieteellisiä ja akateemisia artikkeleita. Yhtä suomenkielistä verkkolähdettä lukuun ottamatta kaikki lähteet ovat englanninkielisiä. Lähteiden hakuun on hyödynnetty Google Scholar, IEEE Xplore ja Springer Nature Link -tietokantoja. Osa lähteistä on löydetty tutkimalla käytettyjen artikkeleiden lähdeluetteloita, ja joitakin lähteitä on löytynyt tieto- ja kyberturvallisuuden asiantuntijoiden verkkosivustoilta. Hakusanoina on toiminut muun muassa “IoT”, “cybersecurity”, “information security”, “CIA-triad” ja “honeypot”.

Tutkielman keskeisenä teemana on tieto- ja kyberturva sekä niiden ulottuvuudet erityisesti esineiden internetin (IoT) kontekstissa. Kodin IoT-laitteet, kuten valvontakamerat, reitittimet, älyvalot, ovat yleistyneet viime vuosina nopeasti, mikä on innostanut kehittäjiä keksimään uusia keinoja helpottamaan arjen yksinkertaisia askareita. Toisaalta älylaitteiden yleistyminen on herättänyt myös kyberrikollisten kiinnostuksen, sillä laitteiden käyttäjäkuntaan kuuluu paljon ihmisiä, joilla on vain rajallisesti tietotekniikan osaamista ja kokemusta tietoturvasta. Tämä yhdistettynä siihen, että valtaosa IoT-laitteiden suojauksesta on joko vakavasti puutteellista tai kokonaan olematonta [3] kasvattaa riskiä joutua kyberhyökkäyksen kohteeksi, joita toteutetaan useammin automatisoiduin menetelmin ja osana laajoja bottiverkkoja.

Tutkielman tavoitteena on selvittää miten hunajapurkkijärjestelmiä (honeypot) voidaan hyödyntää kodin IoT-laitteiden turvallisuuden parantamisessa ja niihin kohdistuvien kyberuhkien havaitsemisessa. Honeypotit ovat tarkoituksella haavoittuvaisiksi naamioituja järjestelmiä, joiden avulla voidaan havaita tietomurtoja, kerätä tietoa hyökkääjien toi-

minnasta ja tutkia hyökkäykseen käytettyjä tekniikoita hallitussa ympäristössä, ilman että varsinainen laite altistuu vaaralle. Tämä tekee hunajapurkkijärjestelmistä tärkeän työkalun ennakoivassa puolustuksessa ja uhkien analysoinnissa. Työn tutkimuskysymykset ovat:

TK 1: Millaiselle perustalle tehokas tietoturva rakentuu?

TK 2: IoT-laitteiden väärinkäytön keinot ja motiivit?

TK 3: Miten hunajapurkkeja hyödynnetään IoT-laitteisiin kohdistuvien kyberiskujen havaitsemiseen?

Tutkielma jakautuu johdantoluvun lisäksi neljään päälukuun. Luvussa 2 käydään läpi kyber- ja tietoturvallisuuden määritelmiä ja eroja. Samassa luvussa tutkitaan CIA-kolmiota (Confidentiality, Integrity, Availability -triad) ja miten nämä tietoturvan kolme peruselementtiä muodostavat perustan vahvalle tietoturvalle. Luku 3 käsittelee hunajapurkkijärjestelmiä, esineiden internetiä (IoT), edellä mainittujen järjestelmien tietoturvaa ja yleisiä riskejä. Luvussa tarkastellaan myös erilaisia IoT-laitteisiin kohdistuvien tietoturvamurtojen kohteita ja motiiveita sekä millaisia tahoja iskujen takana yleensä on. Luku 4 syventyy tutkielman varsinaiseen aiheeseen, eli hunajapurkkijärjestelmien hyödyntämiseen kodin IoT-laitteisiin kohdistuvien hyökkäysiin reagoimiseen, havainnointiin ja tiedonkeruuseen. Pohditaan myös miten murtojen havaitsemisella ja kyberrikollisten toimien seuraamisessa hallitussa ympäristössä voisi parantaa IoT-laitteiden turvallisuutta yleisesti. Lopuksi esitetään yhteenveto aiheista ja niiden merkityksestä IoT-laitteiden tietoturvallisuuden kehittämisessä.

2 Tieto- ja kyberturva

Tietoturva ja kyberturva kuulostavat samanlaisilta, ja monet luulevat, että termit ovat toistensa synonyymejä. On totta, että termien välillä esiintyy päällekkäisyyksiä, mutta myös merkittäviä eroja. Tietoturva (information security) tarkoittaa kaikenlaisen tiedon suojaamista, oli se sitten fyysisessä tai digitaalisessa muodossa. Kyberturvallisuus (cybersecurity) taas keskittyy erityisesti digitaalisen ympäristön uhkiin ja suojautumiseen, kuten verkkoihin, järjestelmiin ja ohjelmistoihin kohdistuviin hyökkäyksiin. Näin ollen kyberturvallisuutta voidaan pitää tietoturvan alaluokkana, joka keskittyy nimenomaan tietoverkkojen ja digitaalisen tiedon suojaamiseen [4]. Tietoturva tarkoittaa tietojen ja tietojärjestelmien suojaamista luvattomalta käytöltä, muutoksilta ja häirinnältä. Se kattaa suojatoimet, jotka estävät tietojen luvattoman muokkauksen tallennuksen, käsittelyn ja siirron aikana sekä palvelunestohyökkäykset (DoS) laillisilta käyttäjiltä. Lisäksi tietoturvaan kuuluu uhkien tunnistaminen, dokumentointi ja torjuminen [5]. Tietoturva on kattotermi, joka käsittelee kaiken tiedon suojaamista luvattomalta pääsyltä, muutoksilta ja tuhoutumiselta riippumatta sen muodosta. Näin ollen tietoturvan historian voidaan katsoa alkaneen jo antiikin ajoista, jolloin tietojen turvaaminen perustui fyysisiin menetelmiin, kuten tietojen sinetöimiseen ja salakirjoitukseen. Esimerkiksi antiikin Roomassa käytettiin Caesarin salakirjoitusta, jossa kirjaimia siirrettiin sovitun määrän aakkosissa viestin salaamiseksi. Tietoturvallisuuden alakäsitteillä on myös mahdollisesti omia alakäsitteitä. Esimerkiksi verkkoturvallisuus (engl. network security) on kyberturvallisuuden osajoukko. Tietoturva on kyberturvaa laajempi käsite ja kattaa sekä fyysisen että digitaalisen tiedon suojauk-

sen CIA-kolmion periaatteiden mukaisesti. Nämä periaatteet varmistavat, että suojattavan tiedon luottamuksellisuus, eheys ja saatavuus säilyvät. CIA-kolmioon palataan myöhemmin. Kyberturvallisuus keskittyy erityisesti digitaalisten tietovarojen suojaamiseen uhkatekijöiltä. Kuten tietoturvassa, sen keskeisenä tavoitteena on turvata tiedon luottamuksellisuus, eheys ja saatavuus. Se suojaa ihmisten, yhteiskunnan ja valtion etuja kyberuhkilta, jotka voivat kohdistua sekä tietoihin että muihin arvokkaisiin resursseihin. Erityisesti kyberturvallisuus keskittyy internetin kautta tapahtuviin hyökkäyksiin ja tietomurtoihin [6]. Tieto- ja kyberturvan välillä vallitsee siis hierarkia: kaikki kyberturva liittyy tietoturvaan, mutta kaikki tietoturva ei ole kyberturvaa. Yhteistä näillä on että molempien rooli modernissa yhteiskunnassa on kriittinen niin yksityishenkilöiden, organisaatioiden kuin kansallisen turvallisuuden kannalta.

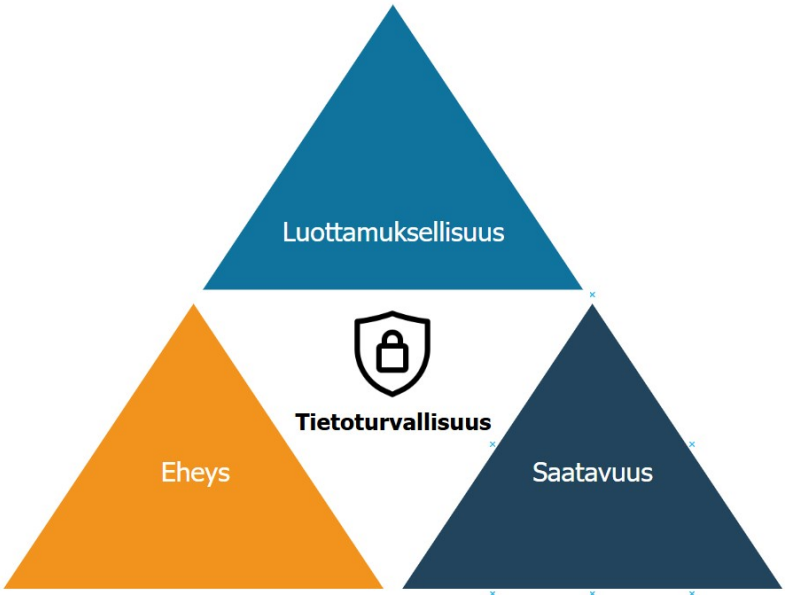
2.1 Kyberturva

Kyberturvallisuuden historia voidaan katsoa alkaneen 1960-luvun lopulla. Vuonna 1969 käynnistettiin Yhdysvaltain puolustusministeriön rahoittama pakettikytkentään (engl. packet switching) perustuva tietoverkko ARPANET (Advanced Research Projects Agency Network). Se mahdollisti ensimmäistä kertaa hajautetun tietojenkäsittelyn ja loi perustan nykyiselle internetille [7]. Sen alkuperäinen tarkoitus oli parantaa eri tutkimuslaitosten välistä kommunikaatiota. Tietoverkko koostui aluksi vain muutamista valtion ja yliopistojen tietokoneista: Verkon käyttäjät olivat tutkijoita ja insinöörejä, jotka luottivat toisiinsa. Tästä johtuen kyber- ja verkkoturvallisuus eivät olleet keskeisessä asemassa ARPANET:in alkuvaiheissa. Vasta myöhemmin havaittiin tarve tietoturvan järjestelmälliselle kehittämiselle, mikä aloitti kyberturvallisuuden systemaatisen tutkimuksen ja käytännön soveltamisen eri aloilla.

Kyberturvallisuus on kokoelma työkaluja, käytäntöjä, turvallisuuskäsitteitä, suojatoimia, ohjeita, riskienhallintamenetelmiä. toimenpiteitä, koulutusta, parhaita käytäntöjä, varmistustoimia ja teknologioita, joita voidaan hyödyntää kyberympäristön sekä organisaatioiden ja käyttäjien etuja [8]. Nämä toimenpiteet tähtäävät eri uhkien havainnointiin, ennakoivaan torjuntaan ja palautumiseen mahdollisista hyökkäyksistä.

2.2 CIA-kolmio

Kestävä tietoturva ja sen alaluokat (esimerkiksi kyber- IT- ja verkkoturvallisuus) [9] [10] rakentuvat vankalle perustalle, joka koostuu kolmesta peruspilarista: **Luottamuksellisuus (Confidentiality)**, **Eheys (Integrity)** ja **Saatavuus (Availability)**. Tätä kolmen peruspe-riaatteen yhdistelmää kutsutaan **CIA-kolmioksi**. Kolmion peruspilarit on esitetty kuvassa 2.1.



Kuva 2.1: CIA (Confidentiality Integrity Availability) -kolmio

- **Luottamuksellisuus (Confidentiality)** tarkoittaa, että tietoihin pääsevät käsiksi vain ne tahot, joilla on oikeudet kyseisiin tietoihin. Esimerkkinä sairaalan potilas-

tietoja pääsevät näkemään ainoastaan sairaalan henkilökunta, jotka tarvitsevat näitä tietoja työnsä suorittamiseksi. Luottamuksellisuus on tiedon suojaamista luvattomilta pääsyiltä ja tietovuodoilta. Luottamuksellisuuden ylläpidon menetelmiä ovat muun muassa:

Salaus (Encryption): Päästä päähän -salaus (End-to-End-encryption) suojaa tiedonsiirtoa alusta loppuun ja estää muita osapuolia pääsemästä tietoihin käsiksi. Esimerkkinä kun lähetetään toiselle viestiä WhatsAppissa, viestit salataan lähettäjän laitteella ja ne voidaan purkaa vain vastaanottajan laitteella. Kolmannet osapuolet ja jopa WhatsAppin omat palvelimet eivät voi lukea viestien sisältöä [11]. Muita salausalgoritmeja ovat muun muassa AES (Advanced Encryption Standard) ja RSA (Rivest, Shamir and Adleman) [12].

Pääsynhallinta (Access control): Pääsynhallinta tarkoittaa järjestelmien, sovellusten ja tietojen käyttöoikeuksien hallintaa siten, että vain valtuutetut henkilöt pääsevät käsiksi tiettyihin resursseihin. Tämä voidaan toteuttaa muun muassa roolipohjaisella pääsynhallinnalla (RBAC, Role-Based Access Control), jolla rajoitetaan verkkoyhteyksiä organisaation käyttäjien roolien perusteella [13].

Tunnistautuminen (Authentication): Tunnistautuminen on prosessi, jonka tarkoitus on varmistaa käyttäjän henkilöllisyys ennen pääsyn sallimista järjestelmään tai tietoihin. Monivaiheinen tunnistautuminen (MFA, Multi-Factor Authentication) lisää ylimääräinen turvakerroksen vaatimalla kahta tai useampaa eri tunnistautumistapaa. Yleisin muoto on kaksivaiheinen tunnistautuminen (2FA, Two-Factor Authentication), jossa esimerkiksi salasanan lisäksi vaaditaan kertäkäyttöinen koodi tai biometrinen tunniste [14].

Tietojen peittäminen (Data masking): Tietojen peittäminen on menetelmä, jolla suojataan arkaluontoisia tietoja piilottamalla ne luvattomilta tahoilta. Tiedot peitellän muokkaamalla alkuperäisiä tietoja niin, että ne säilyttävät hyödyllisyytensä esimerkiksi testauksessa tai analytiikassa, mutta eivät paljasta tiedon

todellisia arvoja. Peittämismenetelmät voivat tarjota eri tasoista suojaa riippuen niiden toteutustavasta ja siitä, kuinka tehokkaasti ne estävät alkuperäisten tietojen rekonstruoinnin [15].

- **Eheys (Integrity)** tarkoittaa sitä, että tieto pysyy muuttumattomana ja todenmukaisena. Eli luvattomat tahot eivät voi muokata tai hävittää jättämättä jälkeä. Tapoja ylläpitää eheyttä ovat muun muassa:

  Versionhallinta: Versionhallinta kirjaa ylös kaikki tiedoissa tapahtuneet muutokset ja mahdollistaa muutosten seuraamisen, mikä on hyödyllistä aiempien versioiden tarkastelussa ja tarvittaessa niiden palauttamisessa.

  Tarkistussumma (Checksum): Tarkistussummat toimivat digitaalisina sormenjälkinä, jotka auttavat havaitsemaan tiedon muutokset vertaamalla nykyistä tarkistussummaa aiempaan versioon.

  Digitaaliset allekirjoitukset: Nämä varmistavat sähköisten asiakirjojen ja verkkosivujen eheyden ja allekirjoittajan aitouden, jotka estävät luvattomien muutosten tekemisen.

- **Saatavuus (Availability)** tarkoittaa, että tiedon tulee aina olla tarvittaessa saatavilla luvallisille tahoille. Ne joilla on oikeudet kyseisiin tietoihin, pääsevät käsittelemään niitä. Saatavuuden varmistaminen edellyttää suojautumista palvelunestohyökkäyksiä vastaan ja varmistamaan, että järjestelmät kestävät häiriötekijöitä. Saatavuuden ylläpitämiseen käytetään muun muassa kuormituksen tasaamista (load balancing), joka tarkoittaa verkkoliikenteen jakamista useammalle palvelimelle. Palautus/toipumissuunnitelmat ovat myös tärkeitä protokollia. Nämä ovat ohjeita, joiden avulla häiriötilanteesta palataan normaaliin toimintaan mahdollisimman sujuvasti.

Näiden kolmen perusperiaatteen lisäksi muita tietoturvan komponentteja ovat **Autenttisuus (Authenticity)** ja **Kiistämättömyys (Non-repudiation)**:

Autenttisuus: Varmuus siitä, että tieto tai viesti on peräisin luotettavasta lähteestä, jolloin vältytään identiteettivarkauksilta, huijauksilta ja väärentämiseltä [16]. Autenttisuuden varmistusmenetelmiä ovat muun muassa tunnistautuminen, jossa käyttäjän identiteetti vahvistetaan esimerkiksi salasanalla tai monivaiheisella tunnistautumisella. Biometrinen tunnistus hyödyntää fyysisiä ominaisuuksia, kuten sormenjälkiä tai kasvonpiirteitä. Esimerkkejä biometrisestä tunnistamisesta löytyy lähes jokaisen taskusta. Nykyään suurimman osan älypuhelimista saa avattua käyttämällä kasvojentunnistusta tai sormenjälkitunnistusta.

Kiistämättömyys: osapuoli ei voi kiistää osallisuuttaan tiedon lähettämisessä/vastaanottamisessa tai tietyn toiminnon suorittamisessa. Tämä on tärkeää varsinkin sähköisessä kaupankäynnissä ja oikeudellisissa asiakirjoissa. Kiistämättömyyden ylläpitoon käytetään **digitaalisia allekirjoituksia**, viestin todennuskoodeja (Message Authentication Code, MAC) ja **aikaleimoja** [17].

2.3 Tekniset toimet tietoturvan parantamiseksi

Tietoturvan tehokas toteuttaminen käytännön tasolla edellyttää ratkaisuja, joilla pyritään estämään tietojen luvaton käyttö ja muokkaaminen, varmistamaan järjestelmien sujuva toiminta ja vähentämään haavoittuvuuksia. Yksi tärkeimmistä tavoista on **palomuuri**, joka säätelee ja valvoo verkkoliikennettä yksityisen verkon ja ulkomaailman välillä. Sen tehtävänä on estää luvattomat pääsyt järjestelmiin [18]. Lisäksi **virustorjuntaohjelmat ja anti-malware-ohjelmistot** havaitsevat ja poistavat haitallisia tiedostoja sekä ehkäisevät niden leviämistä järjestelmässä [19]. Tunkeutumisen havaitsemis- ja estojärjestelmät (Intrusion Detection and Prevention Systems, IDPS) analysoivat järjestelmän ja verkon toi-

mintaa mahdollisten hyökkäysten varalta. Ne voivat joko hälyttää käyttäjää epäilyttävästä toiminnastan tai estää sen automaattisesti [20]. **Salausprotokollat** kuten esimerkiksi SSL (Secure Sockets Layer), TLS (Transport Layer Security) ja HTTPS (Hypertext Transfer Protocol Secure), ovat tärkeitä tiedonsiirron turvaamisessa, sillä ne estävät viestien luvattoman lukemisen ja muokkaamisen niiden siirron aikana [21] [22]. Tietojen **säännöllinen varmuuskopiointi** mahdollistaa tietojen palauttamisen mahdollisten menetysten tai laitevian jälkeen. **Ohjelmiston ja käyttöjärjestelmien säännöllinen päivitys** paikkaavat haavoittuvuuksia, joita hyökkääjät pyrkivät hyväksikäyttämään.

CIA-kolmio on tärkeä ja hyödyllinen malli turvatoimien ja työkalujen arvioimiseen. Jos järjestelmän turvatoimista puuttuu jokin kolmion osa-alueista, järjestelmä on altis haitallisille toimille ja kyberuhille. Jokainen kolmesta peruspilarista on kriittinen tietoturvallisuuden kannalta. Ne toimivat ohjeina ja työkaluina tietomurtojen analysoinnissa sekä turvallisten järjestelmien kehittämisessä. CIA-kolmion periaatteet auttavat organisaatioita kouluttamaan työntekijöitään tietoturvakäytännöissä, ehkäisemään hyökkäyksiä, vahvistamaan suojautumista kyberuhkilta sekä varmistamaan tietojen luottamuksellisuuden, eheyden ja saatavuuden myös kriisitilanteissa.

3 Hunajapurkit ja esineiden internet

Esineiden internetin yleistyminen on muuttanut tapaa, jolla fyysiset laitteet ja järjestelmät kytkeytyvät digitaaliseen maailmaan. Samalla kun arkipäiväiset laitteet kuten ovikellot, jääkaapit ja valvontakamerat liittyvät verkkoon, kasvaa myös kyberuhkien määrä. Hunajapurkit tarjoavat keinon havaita ja ymmärtää näitä uhkia. Ne toimivat ansalaitteina, joiden avulla voidaan seurata hyökkäyksiä ja tunnistaa hyökkääjien toimintatapoja ilman, että varsinaiset tuotantojärjestelmät joutuvat vaaraan. Tässä luvussa tarkastellaan erityyppisiä hunajapurkkeja, niiden soveltuvuutta IoT-ympäristöihin sekä tapoja, joilla niitä voidaan hyödyntää tehokkaasti suojaamaan verkkoon liitettyjä laitteita.

3.1 Hunajapurkit

Hunajapurkkien (engl. honeypots) ensisijainen tehtävä on houkutella kyberrikollisia tunkeutumaan järjestelmään ja kerätä tietoa murtautujien ja järjestelmän kanssakäymisestä, heidän toimintatavoistaan ja työkaluistaan. Saatua informaatiota käytetään hyväksi haavoittuvuuksien paikkaamisessa ja turvajärjestelmien parantamisessa. Samalla todellinen järjestelmä on vahvasti suojattu. Toisin sanoen hunajapurkki on järjestelmä, joka on tarkoituksella suunniteltu näyttämään haavoittuvaiselta ja helposti murrettavissa olevalta kohteelta. Tämä toimii syöttinä hakkereille ja kyberrikollisille, joiden toivotaan lankeavan ansaan. Hunajapurkki näyttää ulkoa päin aivan tavalliselta järjestelmältä, joka sisältää

dataa, sovelluksia ja kaikenlaista informaatiota, jota tyypillisestä järjestelmästä olettaisi löytyvän. Lance Spitzner kuvaili hunajapurkkeja kirjassaan Tracking Hackers (2002) resurssiksi, jolla ei ole tuotannollista arvoa ja jonka hyödyllisyys mitataan sillä, miten tehokkaasti siihen murtaudutaan [1] [23]. Kaikki hunajapurkissa tapahtuva ylimääräinen aktiviteetti ja tietoliikenne mikä tulee hunajapurkkiin ja sieltä ulos viittaa siihen, että sinne on onnistuneesti tunkeuduttu. Haavoittuvuuksia on siis hyvin helppo havaita hunajapurkeissa ja toisin kuin tavanomaisissa tunkeutumisen havaitsemisjärjestelmissä (engl. Intrusion Detection System, IDS), vääriä hälytyksiä (engl. false positive) ei esiinny. [24]

Hunajapurkki on yksittäinen verkkoon liitetty palvelu tai tietokonejärjestelmä, joka toimii syöttinä ja ansana mahdollisille tunkeutujille. Hunajaverkko (engl. Honeynet) taas on useista hunajapurkeista koostuva kokonaisuus, joka houkuttelee hyökkääjiä ja monitoroi heitä useamman järjestelmän kautta. Näitä kahta termiä pidetään usein synonyymeinä, mikä ei periaatteessa ole täysin totta, sillä hunajaverkot ovat huomattavasti monimutkaisempia ja laajempia järjestelmiä kuin yksittäiset hunajapurkit. Edistyneimpien hunajaverkkojen ensisijainen tarkoitus on kerätä kattavaa informaatiota sekä sisäisistä että ulkoisista uhista. Honeypot-järjestelmiä on lukuisia erilaisia ja jokainen eroaa toisestaan lievästi käyttötarkoituksensa mukaan. Kaikkia hunajaverkkoja kuitenkin yhdistää neljä peruselementtiä [25]:

- **Tietojen hallinta (Data control)** tarkoittaa kykyä dokumentoida ja tallentaa tunkeutujan haitallisia toimia.
- **Tietojen kerääminen (Data capture)** tarkoittaa, että aina kun tunkeutuja vuorovaikuttaa järjestelmän kanssa, hunajapurkki seuraa ja tallentaa tapahtumia reaaliajassa. Tämä sisältää muun muassa lokitietojen kirjaamisia, verkon liikenteen seurantaa ja tunkeutujan käyttämien työkalujen dokumentointia.

[1] It's a security resource whose value lies in being probed, attacked, or compromised

- **Tietojen kokoaminen (Data collection)** viittaa kaiken informaation tallentamiseen, mikä tallennetaan hyökkääjän tunkeutumisen aikana. Näitä tietoja säilytetään turvatussa keskitetysti hallitussa lokaatiossa, jotta niiden eheys (integrity) voidaan varmistaa ja ne ovat käytettävissä ilman muuttumisen tai katoamisen riskiä. (ks. CIA-kolmio). Ero tietojen keräämiseen on siinä, että kerääminen tarkoittaa hyökkääjän toiminnan reaaliaikaista tallentamista, kuten edellä mainitut lokitietojen kirjaamiset ja verkon liikenteen seuraaminen, kun taas tietojen kokoaminen keskittyy lähinnä näiden tietojen turvalliseen tallentamiseen ja hallintaan myöhempää analysointia varten.

- **Tietojen analysointi (Data Analysis)** tarkoittaa kaiken tallennetun informaation tarkkaa tutkimista. Tavoitteena on saada selville tietomurron yksityiskohtia, kuten hyökkääjän käyttämiä menetelmiä, strategioita ja mahdollisia tavoitteita. Tämä analyysi on tärkeä vaihe tulevien uhkien torjumiseksi ja suojatoimien parantamiseksi.

Hunajapurkkijärjestelmät voidaan karkeasti jakaa kahteen kategoriaan: Tuotantohunajapurkit (engl. Production honeypots) ja Tutkimushunajapurkit (engl. Research honeypots).

Tuotankohunajapurkit on suunniteltu parantamaan organisaatioiden tuotantoverkon valvontaa ja turvallisuutta. Ne suojaavat ja turvaavat ympäristä, vähentävät hyökkäyksien riskejä ja auttavat ennaltaehkäisemään ja torjumaan hyökkäyksiä. Ne ovat helppoja ottaa käyttöön ja yläpitää, mutta niiden toiminnallisuus on rajoitettu. Tuotantohunajapurkit keräävät vain rajallisesti tietoa hyökkäyksistä [26]. Tyypillisesti ne tarjoavat tietoa ainoastaan hyökkääjien käyttämistä haavoittuvuuksista, mutta eivät paljasta tarkempia yksityiskohtia esimerkiksi käytetyistä työkaluista.

Tutkimushunajapurkkien ensisijainen tarkoitus on selvittää, miten hyökkääjät toteuttavat hyökkäykset ja tutkia heidän käyttämiään menetelmiä. Näitä hunajapurkkeja käyttävät

muun muassa akateemiset tutkijat, tietoturva-asiantuntijat, valtion viranomaiset ja tietoturvayritykset uhkien arvioimiseen [27].

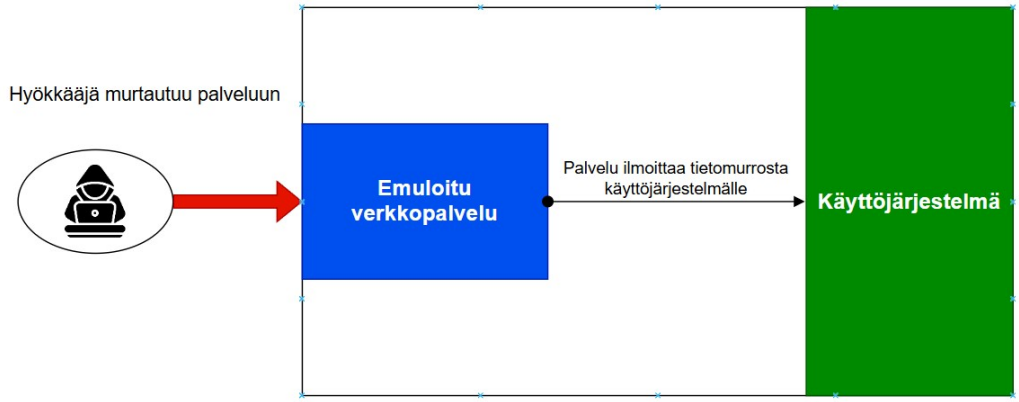
Tuotantohunajapurkkeja voidaan pitää hunajapurkkien lainvalvojina. Samoin tutkimushunajapurkkeja voidaan rinnastaa tiedustelutoimintaan. Niitä käytetään keräämään tietoa rikollisesta toiminnasta, mikä auttaa ymmärtämään paremmin kyberrikollisia – keitä he ovat ja miten he toimivat. Tämän tiedon avulla voidaan kehittää tehokkaampia keinoja suojautua hyökkäyksiltä. Toinen näitä hunajapurkkijärjestelmiä erottava piirre on, että tuotantohunajapurkit lisäävät suoraan arvoa organisaation turvallisuustoimiin. Sen sijaan tutkimushunajapurkit eivät tuo suoraa hyötyä yksittäiselle toimijalle tai organisaatiolle, vaan arvo piilee siitä, että niitä käytetään keräämään tietoa uhista ja valmistautumaan paremmin niitä vastaan [28].

Hunajapurkkijärjestelmät eroavat myös siinä, miten ne otetaan käyttöön, kuinka monimutkaisia harhautukset ovat ja paljonko vuorovaikutusta tapahtuu järjestelmän ja tunkeutujan välillä. Resurssit ja käyttötarkoitus määräävät minkä tason hunajapurkkijärjestelmään kukin organisaatio päätyy investoimaan. Kolme yleistä vaihtoehtoa ovat matalan, keskitason tai korkean vuorovaikutuksen hunajapurkki.

- **Matalan vuorovaikutustason hunajapurkit (low-interaction honeypot)**

  Matalan vuorovaikutustason hunajapurkit ovat yksinkertaisimpia harhautusjärjestelmiä, jotka vaativat vähiten ylläpitoa ja resursseja. Vuorovaikutukset tunkeutujan kanssa ovat vähäisiä ja ne emuloivat rajallisesti joitakin verkkopalveluita tai -protokollia, kuten esimerkiksi SSH (Secure Shell) tai HTTP (Hypertext Transfer Protocol) [29] [30]. SSH on protokolla, jota hyödynnetään etäyhteyksien luomiseen ja hallintaan tietokonejärjestelmien välillä ja HTTP on protokolla, jolla selaimet ja palvelimet välittävät tietoa toisilleen. Emuloitavat palvelimet ovat hyvin yksinkertaisia ja pinnallisia, eivätkä tunkeutujat ole tekemisissä käyttöjärjestelmän kanssa

millään tavalla. Esimerkiksi matalan vuorovaikutuksen ansa voi näyttää ulkoapäin tavalliselta kirjautumissivulta, josta löytyy kentät käyttäjänimelle ja salasanalle, mutta taustalla ei mitään oikeaa toiminnallisuutta. Kun hyökkääjä yrittää kirjautua sisään, hunajapurkki yksinkertaisesti kirjaa ylös tiedot ja ilmoittaa tietoturvatiimille, että järjestelmään on yritetty murtautua. Matalan vuorovaikutuksen hunajapurkit ovat pitkälti vain murtohälyttimiä ja pätevämmät kyberrikolliset saattavat helposti erottaa pinnallisesti samankaltaisen emuloidun palvelimen todellisesta palvelimesta [31] [32]. Matalan vuorovaikutustason hunajapurkin toimintaperiaate on esitetty kuvassa 3.1

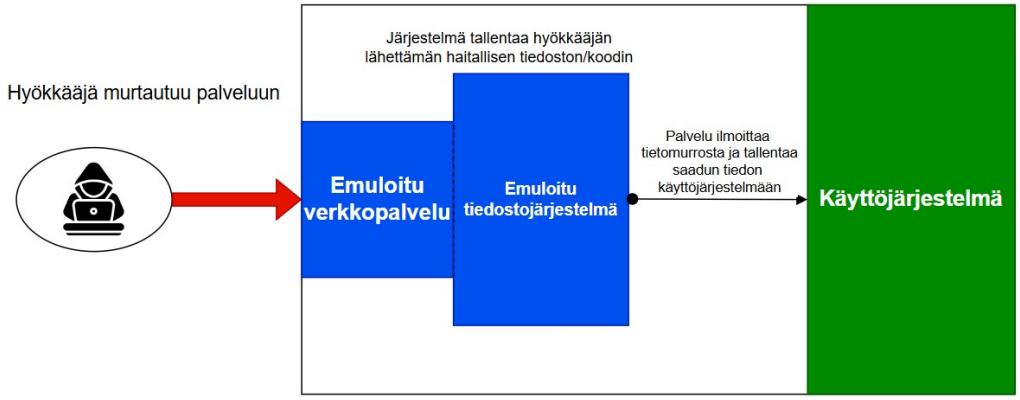


Kuva 3.1: Matalan vuorovaikutustason hunajapurkin toimintaperiaate

- **Keskitason vuorovaikutuksen hunajapurkit (Medium-interaction honeypot)**

  Keskitason vuorovaikutuksen hunajapurkit ovat hieman edistyneempiä kuin matalan vuorovaikutustason ansat, mutta niillä ei edelleenkään ole minkäänlaista käyttöjärjestelmää, jonka kanssa hyökkääjä voisi vuorovaikuttaa. Keskitason vuorovaikutuksen hunajapurkit jäljittelevät esimerkiksi tunnettuja haavoittuvuuksia hyödyntämällä käyttöjärjestelmän TCP/IP-protokollapinoa [33]. Tämä mahdollistaa laajemman vuorovaikutuksen hyökkääjien ja hunajapurkin välillä, mutta niiden toiminta on edelleen rajallista ja ne pystyvät emuloimaan vain tiettyjä haavoittuvuuksia eivätkä kokonaista käyttöjärjestelmää. Keskitason vuorovaikutuksen hunajapurkit eivät kuitenkaan toimi pelkästään murtohälyttiminä, vaan ne pystyvät myös tallentamaan

hyökkääjän lähettämän haitallisen koodin tai tiedoston, mikä auttaa ymmärtämään hyökkääjää paremmin ja tarjoaa syvällisempää tietoa hyökkäyksen luonteesta ja haittaohjelman toimivuudesta [34] [35]. Keskitason hunajapurkin toimintaperiaate on esitetty kuvassa 3.2.

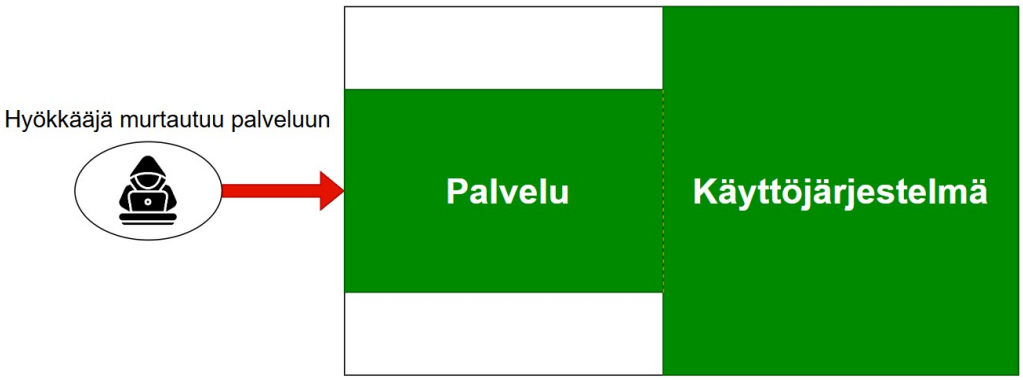


Kuva 3.2: Keskitason vuorovaikutuksen hunajapurkin toimintaperiaate

- **Korkean vuorovaikutustason hunajapurkit (High-interaction honeypot)**

  Korkean vuorovaikutustason hunajapurkit ovat kaikista edistyneimpiä virtuaalisia ansoja. Toisin kuin matalan- ja keskitason vuorovaikutuksen hunajapurkkijärjestelmissä, korkean vuorovaikutustason hunajapurkit tarjoavat hyökkääjille kokonaisia, ulkoapäin haavoittuvaisen oloisia todellisia käyttöjärjestelmiä ja palveluita, joihin he pystyvät tunkeutumaan ja vuorovaikuttamaan sisällön kanssa kuten normaalit, ei-rikolliset käyttäjät. Korkean vuorovaikutuksen hunajapurkkijärjestelmä saattaa koostua tavanomaisesta fyysisestä tietokonejärjestelmistä tai virtuaalikoneista. Virtuaaliset toteutukset ovat käyttöönoton ja hallinnan joustavampia kuin fyysiset [36]. Varsinaisen kyberrikollisen nappaaminen on ylivoimaisesti realistisempaa korkean vuorovaikutustason ansoilla. Hunajapurkin korkean vaikutustason mahdollisuudet tarjoavat ainutlaatuisen näkökulman hyökkääjän liikkeisiin ja toimintaan järjestelmässä. Tosin tämä lisää riskiä, että hyökkääjä kaappaa koko järjestelmän, sillä hunajapurkin ja käyttöjärjestelmän välissä ei ole minkäänlaista erottavaa muuria. Lisäksi hyökkääjät pyrkivät hyödyntämään kaapattuja järjestelmiä uusissa hyökkäyksis-

sä. Haavoittuneita laitteita käytetään roskapostin lähettämiseen tai niillä toteutetaan palvelunestohyökkäyksiä (Denial of Service attack, DoS) [37]. Matalan- ja keskitason ratkaisuihin verrattuna korkean vuorovaikutuksen järjestelmät vaativat huomattavasti enemmän resursseja niin hankintaan kuin ylläpitoon. Korkean vuorovaikutustason hunajapurkkeja on pääasiassa käytetty autonomisesti leviävien haittaohjelmien, kuten matojen, virusten ja bottiverkkojen, kaappaamiseen ja analysointiin [36]. Korkean vuorovaikutus hunajapurkin toimintaperiaate on esitetty kuvassa 3.3



Kuva 3.3: Korkean vuorovaikutustason hunajapurkin toimintaperiaate. Hyökkääjä pääsee varsinaiseen käyttöjärjestelmään käsiksi, sillä palvelun ja käyttöjärjestelmän välillä ei ole mitään erottavaa muuria.

3.2 Esineiden internet

Nykymaailmassa yhä useammat ympäröivät asiat ovat tavalla tai toisella, joko suoraan tai epäsuorasti yhteydessä internetiin. Esineiden internet (engl. Internet of Things, IoT) on osa jokaisen elämää niin kotona kuin ulkonakin, julkisessa liikenteessä, ruokakaupassa ja työpaikalla. Arviolta maailmassa tulee olemaan 25,44 miljardia IoT-laitetta kytkettynä internetiin vuoteen 2030 mennessä [38]. Esineiden internet on verkko, johon liitetyt fyysiset laitteet, ohjelmistot ja anturit keräävät ja jakavat tietoa keskenään. Kotoa löytyviä IoT-laitteita ovat muun muassa erilaiset kodinkoneet ja järjestelmät, joita voi hallita etänä mobiilisovelluksen avulla. Tällaisia laitteita ovat esimerkiksi älyvalot, ovikellot.

Älykoti (smart home) on asunto, jossa laitteita ja järjestelmiä ohjataan langattomasti esimerkiksi älypuhelimella tai älykellolla. Useista kodeista löytyy arjen askareita helpottavia kodinkoneita, kuten robotti-imureita, jotka siivoavat kodin muutamalla napin painalluksella. Hälytysjärjestelmät, kamerat ja liiketunnistimet ilmoittavat käyttäjille reaaliajassa mahdollisista uhista. Wi-Fi:in yhdistetyt älyvalot saa sammutettua vaikka toiselta puolelta maailmaa. Julkisen liikenteen aikataulut näkyvät pysäkeillä olevista näytöistä reaaliajassa. Pysäköintisensorit ilmoittavat vapaat parkkipaikat suoraan sovelluksiin, ja elektroniset hintakyltit sekä älyhyllyt liike- ja painosensoreineen ovat nykyään arkipäivää kaupoissa. IoT on vahvasti läsnä jopa wc-tiloissa, makuuhuoneissa. Sitä hyödynnetään myös aloilla, joiden ei heti arvaisi hyödyntävän huippumodernia, langattomaan verkkoon kytkettyä automatisoitua tekniikkaa, kuten maanviljelyssä [39].

Kyberfyysiset järjestelmät (engl. cyber-physical systems, CPS) ja teollinen internet (engl. Industrial Internet of Things, IIoT) ovat vahvasti läsnä modernissa teollisuudessa ja teknologiassa. IIoT viittaa IoT:n hyödyntämiseen teollisuudessa. Esimerkkejä näistä ovat koneoppiminen ja M2M-viestintä (engl. machine-to-machine-communication). Teollista internettiä hyödynnetään eri teollisuuden aloilla, kuten robotiikassa, lääkintälaitteissa ja ohjelmistopohjaisissa tuotantoprosesseissa. Kyberfyysiset järjestelmät integroivat virtuaalisia palvelujärjestelmiä ja fyysisiä prosesseja. Virtuaalisia järjestelmiä ovat muun muassa laskenta-, viestintä ja ohjausominaisuudet ja fyysinen puoli koostuu laitteista, komponenteista ja antureista, jotka vuorovaikuttavat ympäristönsä kanssa. Teollista internetiä ja samalla asioiden internetiä voidaan oikeastaan pitää kyberfyysisten järjestelmien alaluokkana. IIoT ja IoT keskittyvät fyysisten ”asioiden” yhdistämiseen verkkoon. Kyberfyysisten järjestelmien määritelmä korostaa tietojenkäsittelyn, verkottumisen ja fyysisten järjestelmien integrointia, sisältäen IoT:n ja sen alaluokat [40]. Esimerkkejä kyberfyysisitä järjestelmistä ovat robottiautot, lääkintälaittet, liikenteenhallinta, sähköverkko ja vedenjakelu. Tämä tarkoittaa, että nykyajan infrastruktuuri on hyvin riippuvainen kyberfyysisistä järjestelmistä ja siitä, että kyberpuoli vuorovaikuttaa saumattomasti fyysisten komponent-

tejen kanssa. Nykyään lähes kaikki kriittinen infrastruktuuri on kytköksissä internetiin ja sähköverkkoon, jotka puolestaan ovat alttiita kyberrikollisten ilkivallalle.

3.3 IoT-laitteiden tietoturva ja riskit

IoT-laitteet suunnitellaan käyttäjäystävällisyys edellä, mutta usein samalla tietoturvallisuuden kustannuksella. Vuonna 2020 Palo Alto Networks:in julkaisemassa uhkaraportissa todettiin, että jopa 98 prosenttia Yhdysvaltojen IoT-tietoliikenteestä on salaamatonta [41]. Tämä tarkoittaa, että lähetetävä data siirtyy selkokielisenä kahden pisteen välillä, tässä tapauksessa IoT-laitteen ja esim. pilvipalvelimen, reitittimen tai toisen IoT-laitteen välillä. Tämä tarkoittaa, että kuka tahansa voi nähdä ja lukea dataa, mm. hakkerit, internerpalveluntarjoajat ja valtion viranomaiset.

Salaamattoman tiedon lisäksi monista IoT-laitteista löytyy lisää puutteita tietoturvallisuudessa. Näitä ovat helposti arvattavien oletussalasanojen käyttö, ohjelmistopäivitysten puutteellisuus, avoimet portit, puutteelliset suojausprotokollat sekä heikot käyttöjärjestelmät. Monesti laitteissa ei ole minkäänlaista hallintakäyttöliittymää, eikä käyttäjä ole välttämättä tietoinen siitä onko laite haavoittuvainen vai päivitystä vailla. Vuoden 2024 Netgearin ja Bitdefenderin julkaisemassa tutkimuksessa analysoitiin yli 3,8 miljoonaa kotitaloutta ja 9,1 miljardia tietoturvatapahtumaa vuoden aikana. Kodin IoT-laitteet (älytelevisiot, älypistorasiat, reitittimet jne.) kohtaavat keskimäärin 10 hyökkäystä päivässä. Varsinkin älytelevisiot ovat haavoittuvaisia, sillä niiden elinkaari on suhteellisen pitkä ja valmistajat lopettavat laitetuen ohjelmistopäivityksineen jo muutaman vuoden jälkeen, kun laitteet ovat edelleen käytössä [42]. Käyttäjät eivät usein muista, että he omistavat tiettyjä laitteita. Tästä syystä IP-kamerat, älylamput ja sensorit jäävät pysyvästi verkkoon kuukausiksi tai jopa vuosiksi ilman että niiden ohjelmistoja päivitetään tai turvallisuutta tarkastetaan. Toisin kuin perinteiset IT-laitteet, IoT-laitteisiin kohdistuvat hyökkäykset

vaikuttavat suoraan ympäröivään maailmaan fyysisestikin, kun kriittisen infrastruktuurin järjestelmiä ja terveydenhuollon laitteita voidaan manipuloida etänä.

3.4 Mirai-bottiverkkohyökkäys 2016

Esimerkki laajasta IoT-laitteiden hyväksikäytöstä on **Mirai-bottiverkko**, jota käytettiin kaappaamaan haavoittuvaisia IoT-laitteita, joiden suojaus oli heikkoa tai olematonta (oletustunnukset ja -salasanat). Mirai-haittaohjelma skannasi verkosta löydettäviä laitteita ja kirjautui niihin käyttäen tunnettuja tunnuksia ja salasanoja, jotka oli kovakoodattu itse haittaohjelmaan. Saastuneet IoT-laitteet muuttuvat osaksi bottiverkkoa, joita ohjataan keskitettyjen komentopalvelimien (C&C-palvelimien) kautta. Nämä palvelimet antavat tartuneille laitteille ohjeet mitä kohteita vastaan laitteiden tulee hyökätä seuraavaksi. Mirai siis leviää etsimällä, hyökkäämällä ja tartuttamalla haavoittuvaisia IoT-laitteita, jonka jälkeen laitteista tulee osa haitallista bottiverkkoa. Mirai-bottiverkkoa käytettiin laajoihin palvelunestohyökkäyksiin, joista tunnetuimpia oli hyökkäys DNS-palveluntarjoaja Dyniin lokakuussa 2016. Tämä aiheutti merkittäviä häiriöitä verkkopalveluihin, kuten Amazoniin, Twitteriin, Netflixiin ja GitHubiin [43]. Mirai sai aikaan paljon tuhoa, koska valtaosasta IoT-laitteista puuttui tärkeitä päivityksiä ja ne käyttivät oletussalasanoja, joten bottiverkolla oli runsaasti haavoittuvaisia resursseja käytettävissä. Lisäksi Mirain lähdekoodi julkaistiin pian hyökkäyksen jälkeen verkossa, mikä johti lukuisten varianttien kehittämiseen ja jatkohyökkäysten leviämiseen [44] [45]. Mirai-tapaus osoittaa, miten puutteellinen luottamuksellisuus ja eheys IoT-laitteissa voi johtaa laajamittaiseen hyväksikäyttöön, mikä johtaa palveluiden saatavuuden menettämiseen.

3.5 Motiivit, kohteet ja tekijät

IoT-laitteet vaihtelevat yksinkertaisista sensoreista ja kodin älylaitteista monimutkaisiin teollisuuden koneisiin, joilla kaikilla on omat erityiset ohjelmistot ja laitteisto-ominaisuudet, joten uhkamallit eroavat toisistaan merkittävästi. Ei ole olemassa yhtä tehokasta ainoaa ratkaisua, joka sopisi kaikkiin tilanteisiin. Hyökkääjien motiivit vaihtelevat myös ja ne voidaan jakaa karkeasti neljään pääryhmään. Usein kyse on **taloudellisesta hyödystä**, esimerkiksi kiristyksestä, tietojenkalastelusta (engl. phishing) ja toiseksi henkilöksi tekeytymisestä (engl. spoofing). Taloudellisesti motivoituneet kyberrikolliset saattavat asentaa kiristyshaitaohjelmia älytelevisioihin, valvontakameroihin ja älykelloihin. Nämä haittaohjelmat voivat estää laitteen normaalin käytön tai varastaa arkaluontoista tietoa, kuten henkilötietoja, käyttäjätunnuksia tai tallennettuja videomateriaaleja, ellei käyttäjä maksa vaadittuja lunnaita. Phishing-hyökkäykset kohdistuvat erityisesti käyttäjiin, jotka hallinnoivat IoT-laitteita mobiilisovellusten kautta. Hyökkääjät pyrkivät saamaan selville käyttäjätunnuksia ja salasanoja lähettämällä väärennettyjä huoltoviestejä, tietoturvailmoituksia tai ohjelmistopäivityksiä. Nämä viestit ohjaavat käyttäjän tietojenkalastelusivulle tai asentavat haitallisia sovelluksia, jotka mahdollistavat laitteen etäohjauksen ja pääsyn käyttäjän tietoihin. Spoofing-hyökkäyksillä hyökkääjä esiintyy toisena laitteena tai käyttäjänä päästäkseen käsiksi luottamuksellisiin tietoihin. Kuten esimerkeistä käy ilmi, termien välillä esiintyy päällekkäisyyksiä. **Valtiollinen vakoilu ja sabotaasi** ovat myös yleisiä. Tällöin hyökkäykset kohdistuvat usein kriittiseen infrastruktuuriin, kuten vedenjakeluun, liikenteen ohjaukseen, terveydenhuoltojärjestelmiin tai energiaverkkoihin. IoT-laitteet toimivat porttina esimerkiksi videoneuvottelujärjestelmiin tai muihin arkaluontoisiin tietoverkkoihin. Toisinaan motiiveina ovat myös **ideologiset motiivit** (esim. hacktivismi ja poliittinen vaikuttaminen) ja **demonstratiiviset hyökkäykset**, jossa hyökkääjillä ei ole varsinaista agendaa. Nämä liittyvät pelkkään kokeiluun ja maineen tavoitteluun kyberrikollisten keskuudessa.

Osassa hyökkäyksissä tavoitteena on kaapata IoT-laitteet osaksi laajempaa bottiverkkoa (ks. Mirai-haittaohjelma), jolla toteutetaan palvelunestohyökkäyksiä. Bottiverkkoja voidaan myös käyttää välityspalvelimina (engl. proxy), jolloin hyökkäykset suoritetaan kaapattujen laitteiden kautta. Esimerkiksi hyökkääjä saattaa murtautua järjestelmään bottiverkkoon kuuluvan saastuneen älylaitteen kautta, eikä suoraan omalta koneelta. Tämä vaikeuttaa hyökkäyksen alkuperän jäljittämistä, sillä IP-osoitteet kuuluvat kaapattujen laitteiden omistajille. Viime aikoina bottiverkkoja on hyödynnetty myös kryptovaluuttojen louhimiseen. Louhinta kuluttaa laitteen prosessointitehoa, mikä johtaa kaapatun laitteen suorituskyvyn laskuun ja jopa ylikuumentumiseen. Sähkönkulutus on myös todella suurta, mikä aiheuttaa taloudellista harmia uhrille. Lyhykäisyydessään hyökkäyksiä toteuttavat muun muassa kyberrikollisryhmät, järjestäytyneet rikollisryhmät, valtioilliset tahot ja yksittäiset henkilöt, jotka saattavat tavoittelevat mainetta, poliittisia päämääriä, taloudellista hyötyä tai vaan testata taitojaan käytännön tasolla. Monet kyberhyökkäykset nykyään ovat myös hyvin laajamittaisia ja automatisoituja, jotka käyttävät hyväksi tuhansia haavoittuvaisia laitteita ympäri maailmaa.

Jotta IoT-laitteiden turvallisuutta voidaan parantaa nykytilanteesta, muutokset on aloitettava jo suunnitteluvaiheessa. Kovakoodatut oletussalasanat, salaamaton tiedonsiirto ja heikko ohjelmiston ylläpito muodostavat vakavan tietoturvariskin. Nämä haavoittuvuudet vaativat monitasoisen suojausstrategian, jossa huomioidaan tekniset ja hallinnolliset toimet sekä käyttäjien rooli [46]. Tehokkaita keinoja ovat muun muassa **Sisäänrakennettu tietoturva eli Security by Design**, jossa tietoturva otetaan huomioon jo suunnitteluprosessissa, eikä lisätä vasta jälkikäteen erillisenä ominaisuutena. Myös **tiedonsiirron salaus** on tärkeää. Kaikki laitteen ja palvelimen välillä liikkuva data tulisi salata käyttäen tehokasta salausalgoritmia. Hyvä esimerkki on AES-protokolla (Advanced Encryption Standard), joka sopii varsinkin pienitehoisille kodin IoT-laitteille. **säännölliset ohjelmistopäivitykset** paikkaavat haavoittuvuuksia ja ennaltaehkäisevät niitä hyödyntäviä hyökkäyksiä. Lisäksi **vahva tunnistautuminen ja pääsynhallinta** ovat keskeisiä. Oletussalasanat tulisi vaihtaa

hetimmiten ja ottaa käyttöön monivaiheinen tunnistautuminen (MFA). Ei myöskään pidä unohtaa **käyttäjien riittävää ja säännöllistä kouluttamista**. Laitteiden käyttäjillä tulisi olla perustiedot siitä, kuinka IoT-laitteita käytetään turvallisesti.

Ke Xu ja kollegat (2016) [47] ehdottavat, että tulevaisuuden IoT-turvallisuutta älykodeissa olisi mahdollista parantaa jakamalla ekosysteemi eri toiminnallisiin kerroksiin. Esimerkiksi älylaitteista ja sensoreista koostuvaan laitteistokerrokseen, keskitettyyn hallintaan tarkoitettuun ohjauskerrokseen, sekä ulkoisten palvelujen tajoamiseen keskittyvään palvelukerrokseen. Tällainen **Software Defined Smart Home** mahdollistaa turvallisen ja automatisoidun hallinnan, jossa jokaisella kerroksella on oma roolinsa tiedon käsittelyssä, päätöksenteossa ja palveluiden tarjoamisessa. Pelkkä perinteinen tietoturva-ajattelu ei enää riitä alati kehittyvässä ja hajautetussa IoT-maailmassa. Laitteiden suojaaminen edellyttää kokonaisvaltaista riskienhallintaa, joka ottaa huomioon sekä tekniset että inhimilliset tekijät.

4 Uhkien havainnointi ja ennakoiva puolustus: Hunajapurkit IoT-laitteiden turvallisuudessa

Kyberhyökkäyksten laajuus ja monimuotoisuus varsinkin IoT-laitteitä hyödyntävissä bottiverkoissa osoittavat, kuinka alttiita laitteet ovat väärinkäytöksille. Koska hyökkäykset ovat usein automatisoituja, hajautettuja ja vaikeasti jäljitettävissä, niiden torjuminen vaatii tehokkaita suojaustoimia. Tässä luvussa pohditaan koko tutkielman keskiössä olevaa kysymystä: kuinka honeypot-järjestelmiä voidaan hyödyntää IoT- ja älylaitteisiin kohdistuvien hyökkäysten havaistemisessa ja torjumisessa.

Vaikka tehokkaaseen turvallisuuteen valmistaudutaan jo suunnitteluvaiheessa, pelkkä ennaltaehkäisykään ei yksin riitä estämään hyökkäyksiä. Kyberrikollisten hyökkäystavat kehittyvät jatkuvasti ja nollapäivähaavoittuvuuksia (engl. zero day vulnerabilities) käytetään hyväksi ennen kuin ne ehditään paikkaamaan. Puolustuksen tulee kehittyä jatkuvasti pysyen monta akselta hyökkääjiä edellä. Tämän takia tarvitaan ratkaisuja, jotka estämisen lisäksi myös havaitsevat, analysoivat ja ennakoivat niitä. Yksi tällainen ratkaisu on aiemmin esitelty **hunajapurkkijärjestelmä (engl. honeypot-system)**. Kyseessä on siis tarkoituksella haavoittuvaiseksi tai sellaiseksi naamioitu laite tai palvelu, jonka tarkoitus on houkutella hyökkääjiä ja tarkkailla heidän toimintaasa hallitussa ympäristössä. Hunaja-

purkit eivät ole varsinaisia suojamuureja eivätkä estä hyökkäyksiä kuten esim. palomuurit ja virustorjuntaohjelmat, vaan niiden rooli on havainnoida uhkia ja reagoida niihin. Hunajapurkkien avulla saadaan tietoa hyökkäyksissä käytetyistä työkaluista, komentosarjoista ja siitä, mistä päin maailmaa hyökkäykset tulevat.

4.1 Hunajapurkkien hyödyt IoT-ympäristössä

Kodin IoT-laitteet ovat usein pienitehoisia, joiden laskentateho ja muistimäärä on rajallisia, mikä rajoittaa tiettyjä tietoturvaratkaisuja, kuten ”endpoint-suojaus” ja IPS/IDS eli tunkeutumisen esto- ja tunnistusjärjestelmät, jotka vaativat suuren määrän muistia ja prosessointitehoa. Honeypotit kuuluisi sijoittaa verkkoon itsenäisiksi passiivisiksi työkaluiksi havainnointiin ja ”murtohälyttimiksi”, jotka eivät kuormita laitetta tai muuta infrastruktuuria [48].

IoT-ympäristössä hunajapurkit simuloivat usein laitteita, kuten valvontakameroita, reitittimiä ja älyvaloja. Hyökkäykset kohdistuvat tyypillisesti niiden käyttämiin protokolliin, kuten Telnet, HTTP, SSH ja FTP jne. [48] [49] Hunajapurkit ovat varsinkin silloin hyödyllisiä tilanteissa, jossa varsinaiset IoT-laitteet eivät tallenna lokitietoja eivätkä havaitse hyökkäyksiä. Käytännön tasolla hunajapurkit emuloivat verkkopalveluita, joiden heikkouksia hyökkääjät pyrkivät hyödyntämään. Esimerkiksi **Cowrie** on sekä keskitason että korkean vaikutustason hunajapurkkijärjestelmä, joka pystyy simuloimaan SSH-, Telnet-, SFTP- ja SCP-protokollia. Keskitason järjestelmänä Cowrie kirjaa hyökkääjän komentorivikäskyjä (shell interaction) ja brute force-iskuja simuloidulla UNIX-järjestelmällä emuloimalla useita komentoja. Korkean vuorovaikutustason järjestelmänä se toimii välityspalvelimena (proxy) SSH- ja Telnet-yhteyksille, joka mahdollistaa hyökkääjän toiminnan tarkkailun taustajärjestelmään liitetyillä virtuaalikoneilla [48].

Hunajapurkkien avulla saadut tiedot paljastavat mitä portteja ja palveluita hyökkääjät kar-

toittavat ja millä tavoilla he yrittävät murtautua järjestelmiin. Toiseksi lokitietoihin kirjatut komennot, IP-osoitteet ja haitalliset tiedostot voidaan analysoida jälkikäteen esimerkiksi koneoppimismalleilla [50] [51] ja välittää eteenpäin kyberturvallisuusviranomaisille.

4.2 Hunajapurkkien havaitsemat hyökkäystekniikat

Hunajapurkkijärjestelmien keskeinen tehtävä on tarkkailla hyökäysten käytännön toteutusta eli mitä portteja rikolliset skannaavat, mitä komentoja suoritetaan ja miten he pyrkivät etenemään järjestelmässä. Hunajapurkit ovat varsinkin tehokkaita paljastamaan toistuvia ja automatisoituja hyökkäystekniikoita. **Brute force -hyökkäykset** ovat yksi yleisimmistä menetelmistä, jotka kohdistuvat varsinkin SSH- ja Telnet-palveluihin. Tarkalleen ottaen noin 70 prosenttia kaikista IoT-laitteisiin kohdistuvista iskuista ovat nimenomaan brute force hyökkäyksiä näihin kahteen palveluun, sillä ne tyypillisesti käyttävät tunnettuja oletussalasanoja [52] [53].

Porttiskannaus on toinen yleinen tekniikka, jossa hyökkääjä kartoittaa järjestelmän portteja ja etsii avoimia portteja ja tarkistaa, mitä palveluita niissä on käynnissä. Tämä on yleensä ensimmäinen askel ennen varsinaista hyökkäystä. Nmap on yleinen työkalu tähän tarkoitukseen.

Kolmas merkittävä hyökkäystekniikka liittyy bottiverkkojen rakentamiseen. Hyökkääjät pyrkivät asentamaan haitallisen ohjelmiston suojaamattomaan laitteeseen, jotka sitten liittävät laitteen osaksi suurempaa bottiverkkoa, joka voi koostua tuhansista kaapatuista IoT-laitteista (ks. Mirai-bottiverkko. Hunajapurkkien tallentamissa lokitiedoissa näkyy usein komentoja kuten ”wget” ja ”cURL”, joilla ladataan verkosta haitallisia ohjelmia laitteeseen (cURL:ia käytetään myös tiedostojen lähettämiseen), sekä ”chmod”, joka muuttaa tiedostojen käyttöoikeuksia. Näillä komennoilla haitallinen skripti ladataan, tehdään siitä suorituskelpoinen ja käynnistetään saastuneessa IoT-laitteessa. [54].

Bottiverkot pyrkivät muodostamaan pysyviä yhteyksiä komentopalvelimiin (C2, Command & Control), joiden kautta bottiverkon laitteiden hallinta ja kommunikaatio tapahtuu. Korkean vaikutustason hunajapurkkijärjestelmien avulla on mahdollista havaita nämä C2 hyökkäystekniikat ja analysoida niissä käytettyjä IP-osoitteita sekä protokollia.

Zhou ja kollegat (2019) [55] ovat kehittäneet **Chameleon**-nimisen adaptiivisen hunajapurkkijärjestelmän, joka kykenee simuloimaan laajaa joukkoa erilaisia IoT-laitteita. Chameleon koostuu useasta erillisestä komponentista, kuten ”front-end-responderista”, joka vastaa verkkopyyntöihin, ”back-end-interactorista”, joka hallinnoi todellisia yhteyksiä laitteisiin ja evaluator-moduulista, joka varmistaa toiminnan turvallisuuden. Chameleon on suunniteltu estämään sormenjälkitunnistamista (fingerprinting) hyökkääjien toimesta, mikä on suurempi riski esimerkiksi Honeyd-, Dionaea ja Conpot-hunajapurkilla. Sen sijaan että vastaukset olisivat kiinteitä ja epäilyttäviä hyökkääjän silmissä, Chameleon generoi vastaukset dynaamiseseti vastaamaan todellista laitteen palauttamaa dataa. Tämän ansiosta hyökkääjä ei saa selville, että kyseessä on hunajapurkkiansa. Arviointivaiheessa testattiin Chameleon järjestelmää käyttäen hyväksi Honeyscore-työkalua, joka pyrkii tunnistamaan hunajapurkkijärjestelmät. Chameleon kykeni onnistuneesti naamioimaan itsensä IP-kameroiksi, reitittimiksi ja PLC-laitteiksi eikä Honeyscore tunnistanut laitteita hunajapurkkijärjestelmän simulaatioiksi. Näiden ominaisuuksien ansioista Chameleon soveltuu mainiosti pitkäkestoiseen hyökkäysten havainnointiin varsinkin heterogeenisissä ja resurssirajoitteisissa IoT-ympäristöissä [48].

4.3 Hunajapurkkien haasteet ja mahdolliset tulevaisuuden kehityssuunat

Vaikka hunajapurkit ovat tehokkaita työkaluja IoT-laitteisiin kohdistuvien kyberhyökkäysten havainnointiin ja tiedon keräämiseen, niiden käyttöönottoon ja ylläpitoon liittyy haasteita, niin teknisiä että eettisiä. Yksi näistä haasteista liittyy hunajapurkkien vuorovaikutustasoon. Matalan- ja keskitason järjestelmät simuloivat rajoitetusti palveluita ja varsinkin kokeneemmat hyökkääjät osaavat erottaa nämä järjestelmät helposti varsinaisista laitteista [56]. Korkean vuorovaikutustason järjestelmät taas tarjoavat hyökkääjälle aidon käyttöjärjestelmän jonne tunkeutua, mutta niiden jatkuva käyttö sekä ylläpito vaativat jatkuvaa valvontaa ja resursseja, jotta niistä itsessään ei muodostuisi tietoturvariskiksi.

Toinen ongelma on havaittavuus. Hyökkääjät saattavat tunnistaa emuloituja palveluita ja virtuaalikonejärjestelmiä hyödyntäviä hunajapurkkeja esimerkiksi omituisilla vasteajoilla tai puuttuvilla käyttöjärjestelmätiedoilla. Erityisesti asiakaspuolen hunajapurkit (client honeypots), jotka etsivät aktiivisesti haitallisia verkkosivuja, saattavat joutua sormenjälkitunnistuksen uhriksi. Hyökkääjät saattavat käyttää CAPTCHA-testejä paljastakseen hunajapurkkijärjestelmän [57].

Kolmas ongelma liittyy laillisiin ja eettisiin kysymyksiin. Hunajapurkin käyttäjä saattaa joutua vastuuseen, jos järjestelmä itsessään saastuu ja sitä hyödynnetään kyberhyökkäyksiin muihin kohteisiin. Riski on suuri varsinkin korkean vuorovaikutustason järjestelmissä, sillä hyökkääjä saa tällöin kaapattua omaan käyttöön kokonaisen laitteen järjestelmineen, eikä varashälytintä tai IP-osoitteen keräämiseen tarkoitettua pinnallista ansaa.

Herää myös kysymys, missä määrin kyberuhilta puolustautuminen oikeuttaa hyökkääjien toiminnan tarkkailun. Spitznerin (2002) mukaan hunajapurkit tarjoavat arvokasta tietoa hyökkääjien toimintatavoista ja motiveista [23], mikä tukee niiden käyttöä puolustuksel-

lisena työkaluna. Bringerin (2012) mukaan alalla ei ole saavutettu laajasti hyväksyttyä yksimielisyyttä siitä, millainen hunajapurkkien käyttö on laillisesti ja eettisesti sallittua, etenkin yksityisessä käytössä [58]. Monet korkean vuorovaikutustason hunajapurkit kykenevät esimerkiksi tallentamaan hyökkääjien henkilökohtaisia tietoja, joka jakaa mielipiteitä ja herättää kysymyksiä yksityisyydensuojasta.

Yksityishenkilön tai organisaation vastuu hunajapurkkien käytöstä korostuu varsinkin tilanteissa, joissa korkean vuorovaikutustason hunajapurkkien suojaus pettää ja toimii huomaamatta hyökkäysten alustana muihin kohteisiin [37]. Tällaiset tilanteet tuovat esille kysymyksiä hunajapurkkien säännöstelyn tarpeellisuudelle ja oikeudellisille linjauksille, jotka ottavat huomioon sekä tietoturvan että yksityisyydensuojan näkökulmat.

Nykyiset hunajapurkkijärjestelmät toimivat usein erillisinä ja staattisina yksikköinä. Nämä ansat vaativat manuaalista ylläpitoa ja tulosten analysointia [59]. Tulevaisuudessa voisi kehitellä hajautettuja, pilvipohjaisia ja keskenään kommunikoivia hunajapurkkiverkostoja, jotka hyödyntävät lohkoketjuteknologiaa (blockchain) ja koneoppimista. Nämä järjestelmät olisivat tehokkaampia, sillä useat laitteet tekevät samanaikaisesti havaintoja sekä kirjaavat ylös lokitietoja, mikä parantaa sekä hyökkäysten havaitsemisen kattavuutta että skaalautuvuutta. Nishad ja Singh (2024) [60] esittävät ratkaisun, jossa lohkoketjuteknologiaa käytetään hajautetun hunajapurkkijärjestelmän perustana. Heidän mallissaan jokainen hunajapurkkisolmu rekisteröityy verkkoon älysopimusten (smart contracts) avulla, joka julkaisee konfiguraationsa lohkoketjuun ja osallistuu laitteiden väliseen tiedonvaihtoon ilman keskitettyä laitehallintaa. Lisäksi lohkoketjupohjainen lokijärjestelmä varmistaa, että tapahtumat pysyvät muuttumattomina (ks. CIA-kolmion eheys).

Lim ja kollegat (2014) [61] esittelevät saman suuntaista kehitystä, jossa hyödynnetään **Raspberry Pi** -mikrotietokoneita hajautetuina hunajapurkkiantureina, jotka keräävät tietoa reaaliajassa ja lähettävät havainnot keskitettyyn tietokantaan. Kyseisessä järjestelmässä käytetään matalan vuorovaikutustason **Dionaea**-hunajapurkkia, joka emuloi seitsemää

tunnettua verkkopalvelua (SMB, HTTP, MySQL, MSSQL, FTP, TFTP ja SIP) ja vastaanottaa kyberhyökkäyksiä tarkoituksellisesti haavoittuvilta porteilta. Jokainen Raspberry Pi -yksikkö lähettää hyökkäyksessä saamansa tiedon reaaliajassa keskuspalvelimelle XMPP-protokollaa (Extensible Messaging and Presence -Protocol) käyttäen. Kuten aiemmin mainitussa lohkoketjuratkaisussa, Tämän arkkitehtuurin etuna ovat skaalauttavuus ja kustannustehokkuus. Raspberry Pi -mikrotietokoneet ovat edullisia ja energiatehokkaita. Näin ollen niitä voidaan hyödyntää laajemmin eri verkoissa ja sijoitella ympäri maailmaa osaksi laajempaa **hunajaverkkoa** (ks. kolmas luku), jolloin kattavuus paranee huomattavasti. Tämä mahdollistaa myös tietojen tarkemman dokumentoinnin, kuten hyökkäysten alkuperämaat, käytetyt haittaohjelmat ja kohdeportit, mikä tarjoaa arvokasta tietoa sekä tutkimus- että kehityskäyttöön. Tällaiset hajautetut järjestelmät voisivat hyötyä merkittävästi koneoppimisesta ja automatisoidusta uhka-analytiikasta, jolloin järjestelmät eivät rajoittuisi pelkästään hyökkäysten tarkkailuun, kykenisivät myös oppimaan hyökkäyksistä ja ennakoimaan niitä tehokkaammin.

Yksityishenkilöiden ja pienempien organisaatioiden näkökulmasta hunajapurkkien käyttö voisi tuoda sekä mahdollisuuksia että riskejä. Hunajapurkit ovat arvokkaita oppimisympäristöjä, sillä ne auttavat käyttäjää ymmärtää paremmin verkon kautta tulevia uhkia ja kykenevät paljastamaan esimerkiksi IoT-laitteisiin kohdistuvia brute force -hyökkäyksiä, tiettyjä haittaohjelmia sekä haavoittuvaisien porttien skannauksia.

Kotikäyttöön soveltuvat varsinkin kevyemmät, käyttäjäystävälliset ja avoimen lähdekoodin hunajapurkit, kuten **Cowrie**, **Dionaea** ja **T-Pot**. Näiden hunajapurkkien käyttöön ottaminen on suhteellisen helppoa, ja ne antavat konkreettisia tuloksia ja tietoja hyökkäysyrityksistä. Toisaalta niin yksinkertaisia kuin hunajapurkkien käyttäminen saattaa olla, ne vaativat käyttäjältä tietyn verran tietoturvaosaamista. Pelkkä lokien tulkinta vaatii ainakin keskitason tietotekniikan osaamista. Mahdolliset järjestelmien väärät konfiguraatiot saattavat johtaa siihen, että varsinainen järjestelmä saastuu ja joutuu esimerkiksi osak-

si bottiverkkoa, tulevaisuuden palvelunestohyökkäysten välikappaleeksi. Tässä korostuu käyttäjän oma vastuu hunajapurkkien käytöstä, sillä useasti käyttäjä on tietämätön siitä, että oma laite on saastunut ja käyttäjän laitetta ja näin olen myös IP-osoitetta käytetään muiden laitteiden kimppuun hyökkäämiseen.

Vaikka hunajapurkit keräävät arvokasta tietoa hyökkäystilanteista, niiden hyödyntäminen vaatii strategista ajattelua. IoT-ympäristössä olisi järkevintä asentaa useita kevyitä, erilaisia protokollia emuloivia hunajapurkkijärjestelmiä eri verkkoalueille, jolloin voidaan kattaa laajempi hyökkäyspinta-ala. Tämän lisäksi olisi hyvä, jos lokitietojen keräämisen lisäksi hunajapurkki olisi osa laajempaa torjuntastrategiaa, joka kattaa tehokkaan reagoinnin ja tietojen analysoinnin.

Tulevaisuudessa IoT-laitteiden käyttäjien tietotekniikan yleisosaamiseen ja tietoisuuteen riskeistä tuli panostaa tehokkaammin. Valmiiksi kovennetut, helppokäyttöiset ja aloittelijaystävälliset hunajapurkkialustat olisivat mainio lisäpalvelu tavallisille kuluttajille perinteisten palomuurien ja virustorjuntaohjelmien kylkeen. Nämä hunajapurkit auttavat laitteiden käyttäjiä havaitsemaan poikkeavaa liikennettä omissa verkoissaan ja saada konkreettista näyttöä siitä, kuinka usein heidän IoT-laitteensa altistuvat ulkoisille uhille. Tämä lisää omalta osaltaan tietoisuutta IoT-laitteiden riskeistä ja mahdollisesti kannustavat laitteiden valmistajia panostamaan enemmän kestävään tietoturvan ja ohjelmistojen ylläpitoon.

Kaikki edellä mainitut toimet vaativat kuitenkin lainsäädännöllisiä ja eettisiä linjauksia siitä, kuinka hunajapurkeilla kerättyjä tietoja voidaan hyödyntää ja kuka on vastuussa sen hallinnasta. Kynnystä ottaa hunajapurkkijärjestelmiä käyttöön voisi madaltaa tarjoamalla valmiita hunajapurkkialustoja osana tietoturvapaketteja, jolloin tavalliset kuluttajat pystyvät ottaa niitä vaivattomasti käyttöön jopa ilman syvällisempää teknistä osaamista.

Lopuksi hunajapurkit eivät yksin takaa suojaa, koska ne eivät itsessään estä hyökkäyksiä. Hunajapurkit eivät toimi suojamuureina tietomurtoja vastaan, vaan niitä tulisi käyttää vi-

rustorjuntalaitteiden ja palomuurien rinnalla. Niiden arvo riippuu siitä, kuinka hyvin ne onnistuvat houkuttelemaan hyökkääjiä ja kuinka tehokkaasti hyökkääjien tavoista ja työkaluista kerättyä tietoa osataan hyödyntää IoT-laitteiden tietoturvallisuuden parantamisessa [23].

5 Yhteenveto

Esineiden internet on tullut jäädäkseen. Sekä kodin että teollisuuden IoT-laitteet ovat helpottaneet ihmisten jokapäiväistä elämää, tehostaneet yhteiskunnan toimintaa ja tehneet yksitoikkoisista arjen askareista vaivattomampia. IoT-laitteiden nopea yleistyminen on tuonut runsaasti uusia mahdollisuuksia, mutta myös avanut ovia uusille riskeille, joita ei ole huomioitu riittävän hyvin. Tässä kandidaatintutkielmassa on tarkasteltu, kuinka hunajapurkkijärjestelmiä voidaan hyödyntää kodin IoT-laitteisiin kohdistuvien kyberuhkien havaitsemisessa ja tutkimisessa. Hunajapurkit eivät ole perinteisiä viruksentorjuntaohjelmistoja, jotka ovat suurimmalle osalle ihmisistä tuttuja, vaan ne tarjoavat ainutlaatuisen keinon tarkkailla kyberrikollisten toimintaa hallitussa ympäristössä, ilman että varsinaiset laitteet altistuvat vaaralle.

Tutkimuksen perusteella voidaan päätellä, että hunajapurkkijärjestelmät ovat hyödyllisiä varsinkin esineiden internetin kontekstissa. Näiden laitteiden tietoturvallisuus ei ole tarpeeksi kattavaa. Sovelluspäivityksiä tulee harvoin, jos koskaan. Laitteita käytetään useita vuosia sen jälkeen kun valmistaja lopettavat käyttöjärjestelmän ylläpidon, joka asettaa laitteet suurelle vaaralle joutua kaapatuksi. Hunajapurkit toimivat passiivisina murtohälyttiminä. Niiden avulla voidaan havaita hyökkäyksiä, joita ei muuten olisi ehkä koskaan huomattu. Esimerkkejä ovat brute force -hyökkäykset oletussalasanoja hyödyntäen, saastuneiden laitteiden liittäminen osaksi bottiverkkoa tai komentopalvelinyhteyksiä. Lisäksi hunajapurkit tarjoavat arvokasta tietoa haitallisista koodeista, IP-osoitteista ja protokollis-

ta, joita hyväksi käyttäen voidaan kehittää kestävämpiä ja tehokkaampia suojausmekanismeja tulevaisuudessa. Tutkielma osoittaa myös, että vaikka hunajapurkit ovat tehokkaita uhkien havaitsemisessa, ne eivät suoraan estä hyökkäystä, mutta voivat tarjota hyötyä torjuntaan jatkossa. Hunajapurkkeja tulisi käyttää osana vankkaa kyberturvastrategiaa yhdessä muiten puolustusmekanismien, kuten virtustorjuntaohjelmistojen, säännöllisten päivitysten ja palomuurien kanssa. Lisäksi korkean vuorovaikutustason hunajapurkit tuovat mukanaan omat tekniset ja eettiset haasteensa.

5.1 Vastaukset tutkimuskysymyksiin

TK 1: Millaiselle perustalle tehokas tietoturva rakentuu?

Tehokas tietoturvallisuus rakentuu CIA-kolmion kolmeen peruspilariin: luottamuksellisuuteen, eheyteen ja saatavuuteen. Näitä tukevat tiedon autenttisuus ja kiistämättömyys. Eli vain valtuutetut tahot saavat nähdä tiedon, tiedon tulee pysyä muuttumattomana ja luotettavana sekä tiedon tulee olla käytettävissä silloin, kun sitä tarvitaan. Turvallisuusratkaisut, kuten salaus (encryption), pääsynhallinta, tarkistussummat ja hajautettujen palvelunestohyökkäysten (DDoS) torjunta, muodostavat vankan perustan tehokkaalle suojaukselle. IoT-ympäristössä näiden ratkaisujen on oltava kevyitä ja joustavia, jotta niitä voidaan hyödyntää laitteissa, joilla on rajalliset resurssit.

TK 2: IoT-laitteiden väärinkäytön keinot ja motiivit?

IoT-laitteita valjastetaan muun muassa bottiverkkoihin, henkilötietojen kalasteluun, kiristyksiin, vakoiluun ja kryptovaluutan louhintaan. Motiiveina ovat taloudelliset hyödyt, poliittinen vaikuttaminen, ideologiset syyt tai yksinkertaisesti halu testata taitojaan ja saavuttaa mainetta kyberrikollisten keskuudessa. Laitteiden puutteellinen suojaus ja käyttä-

jien puutteellinen tietämys tietoturvasta mahdollistavat hyökkäysten laajan mittakaavan ja tekevät IoT-ympäristöstä houkuttelevat kohteen vihamielisille tahoille.

TK 3: Miten hunajapurkkeja hyödynnetään IoT-laitteisiin kohdistuvien kyberiskujen havaitsemiseen?

Hunajapurkit emuloivat haavoittuvaisia IoT-laitteita ja palveluita tarkoituksenaan houkutella hyökkääjiä. Ne tallentavat hyökkäysyritykset lokitietoihin, kuten esimerkiksi brute force -hyökkäykset ja haittaohjelmien lataukset, jotka mahdollistavat hyökkääjien toimintatapojen analysoinnin jälkikäteen. Tämän avulla voidaan syventää ymmärrystä rikollisten tavoista ja kehittää IoT-laiteiden tietoturvallisuutta entistä tehokkaammaksi.

Mirai-bottiverkkohyökkäys vuodelta 2016 on hyvä esimerkki siitä, mihin puutteellinen luottamuksellisuus ja eheys voivat johtaa. Miljoonat IoT-laitteet saastutettiin haittaohjelmilla, niistä muodostettiin bottiverkko ja niitä käytettiin laajoihin palvelunestohyökkäyksiin, joiden vaikutukset tuntuivat maailmanlaajuisesti. Tapaus toimii malliesimerkkinä sille, miten pienetkin aukot tietoturvallisuudessa voivat eskaloitua globaaleiksi uhiksi. Tietoturvan perusperiaatteiden laiminlyönti, kuten esimerkiksi heikkojen salasanojen ja salaamattomien yhteyksien käyttäminen voivat johtaa suoraan järjestelmien saatavuuden menettämiseen.

5.2 Jatkotutkimusaiheet

Tulevaisuudessa aihetta voisi syventää kehittämällä tehokkaampia, tekoälyyn ja koneoppimiseen perustuvia analyysimenetelmiä, jotka käsittelevät reaaliajassta hunajapurkeista kerättyjä tietoja ja tunnistavat poikkeavuuksia entistä tarkemmin. Vertaileva tutkimus eri vuorovaikutustasojen hunajapurkkijärjestelmien tehokkuudesta erilaisissa ympäristöissä tarjoaisi arvokasta tietoa esimerkiksi siitä, millaiset turvatoimet ja ratkaisut toimivat par-

haiten resurssirajoitteisissa IoT-laitteissa. Kestävä tieto- ja kyberturvallisuus edellyttää jatkuvaa kehitystä, niin IoT-ympäristössä kuin tietotekniikan alalla yleisellä tasolla. Hunajapurkit ovat oikea askel kohti ennakoivampaa, älykkäämpää ja tehokkaampaa esineiden internetin suojaamista.

Lähdeluettelo

[1] M. Warner, ”Cybersecurity: A pre-history”, *Intelligence and National Security*, vol. 27, nro 5, s. 781–799, 2012.

[2] G. Bassett, C. D. Hylender, P. Langlois, A. Pinto ja S. Widup, ”Data breach investigations report”, *Verizon DBIR Team, Tech. Rep*, s. 6–8, 2021.

[3] T. Sasi, A. H. Lashkari, R. Lu, P. Xiong ja S. Iqbal, ”A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms and challenges”, *Journal of Information and Intelligence*, vol. 2, nro 6, s. 455–513, marraskuu 2024, ISSN: 2949-7159. DOI: 10.1016/j.jiixd.2023.12.001.

[4] R. Reid ja J. Van Niekerk, ”From information security to cyber security cultures”, teoksessa *2014 Information Security for South Africa*, 2014, s. 1–7. DOI: 10.1109/ISSA.2014.6950492.

[5] A. Jones ja G. L. Kovacich, *Global information warfare: The new digital battlefield*. CRC Press, 2015.

[6] B. Von Solms ja R. Von Solms, ”Cybersecurity and information security–what goes where?”, *Information & Computer Security*, vol. 26, nro 1, s. 2–9, 2018.

[7] M. Eling, M. McShane ja T. Nguyen, ”Cyber risk management: History and future research directions”, *Risk Management and Insurance Review*, vol. 24, nro 1, s. 93–125, maaliskuu 2021, ISSN: 1540-6296. DOI: 10.1111/rmir.12169.

[8] P. M. Datta, ”Introduction to Cybersecurity”, teoksessa *Global Technology Management 4.0*. Springer International Publishing, 2022, s. 145–153, ISBN: 9783030969295. DOI: 10.1007/978-3-030-96929-5_9.

[9] A. Alexei ja A. Alexei, ”The Difference between Cyber Security vs Information Security”, *Journal of Engineering Science*, vol. 29, nro 4, s. 72–83, tammikuu 2023, ISSN: 2587-3482. DOI: 10.52326/jes.utm.2022.29(4).08.

[10] J. Wang, *Computer Network Security*. Springer Berlin Heidelberg, 2009, ISBN: 9783540796985. DOI: 10.1007/978-3-540-79698-5.

[11] K. Ermoshina, F. Musiani ja H. Halpin, ”End-to-end encrypted messaging protocols: An overview”, teoksessa *Internet Science: Third International Conference, INSCI 2016, Florence, Italy, September 12-14, 2016, Proceedings 3*, Springer, 2016, s. 244–254.

[12] A. Hamza ja B. Kumar, ”A review paper on DES, AES, RSA encryption standards”, teoksessa *2020 9th International Conference System Modeling and Advancement in Research Trends (SMART)*, IEEE, 2020, s. 333–338.

[13] VPNUNLIMITED, *Mikä on roolipohjainen käyttöoikeuksien hallinta (RBAC) - Kyberturvallisuuden termit ja määritelmät*. url: https://www.vpnunlimited.com/fi/help/cybersecurity/rbac?srsltid=AfmBOooti9zfySDeXVdX3r_yVr2Iej4Tlg8i4uGqPegHQRcIaUvEuaBs (viitattu 31. 03. 2025).

[14] Kyberturvallisuuskeskus, *Monivaiheinen tunnistautuminen suojaa käyttäjätilejäsi | Kyberturvallisuuskeskus — kyberturvallisuuskeskus.fi*, https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/monivaiheinen-tunnistautuminen-suojaa-kayttajatilejasi, (Viitattu 15.03.2025).

[15] G. Duncan ja L. Stokes, ”Data masking for disclosure limitation”, *Wiley Interdisciplinary Reviews: Computational Statistics*, vol. 1, nro 1, s. 83–92, 2009.

[16] A. Haider ja A. Koronios, ”Authenticity of Information in Cyberspace: IQ in the Internet, Web, and e-Business.”, tohtorinväitöskirja, Massachusetts Institute of Technology, 2003.

[17] S. Abidin, V. R. Vadi ja A. Rana, ”On confidentiality, integrity, authenticity, and Freshness (CIAF) in WSN”, teoksessa *Advances in Computer, Communication and Computational Sciences: Proceedings of IC4S 2019*, Springer, 2021, s. 87–97.

[18] Kaspersky, *What is a Firewall? How Firewalls Work & Types of Firewalls*. url: https://www.kaspersky.com/resource-center/definitions/firewall (viitattu 31. 03. 2025).

[19] C. Rohith ja G. Kaur, ”A Comprehensive Study on Malware Detection and Prevention Techniques used by Anti-Virus”, teoksessa *2021 2nd International Conference on Intelligent Engineering and Management (ICIEM)*, 2021, s. 429–434. DOI: 10.1109/ICIEM51511.2021.9445322.

[20] D. Mudzingwa ja R. Agrawal, ”A study of methodologies used in intrusion detection and prevention systems (IDPS)”, teoksessa *2012 Proceedings of IEEE Southeastcon*, 2012, s. 1–6. DOI: 10.1109/SECon.2012.6197080.

[21] R. Oppliger, *SSL and TLS: Theory and Practice*. Artech House, 2023.

[22] digicert, *What is SSL, TLS and HTTPS? | DigiCert*, en-US. url: https://www.digicert.com/what-is-ssl-tls-and-https (viitattu 31. 03. 2025).

[23] L. Spitzner, *Honeypots: Tracking Hackers*. Boston: Addison-Wesley, 2002.

[24] C. Seifert, I. Welch, P. Komisarczuk et al., ”Honeyc-the low-interaction client honeypot”, *Proceedings of the 2007 NZCSRCS, Waikato University, Hamilton, New Zealand*, vol. 6, s. 48, 2007.

[25] N. Titarmare, N. Hargule ja A. Gupta, ”An overview of honeypot systems”, *International Journal of Computer Sciences and Engineering*, vol. 7, nro 2, s. 394–397, 2019.

[26] G. Ikuomenisan ja Y. Morgan, ”Meta-Review of Recent and Landmark Honeypot Research and Surveys”, *Journal of Information Security*, vol. 13, nro 04, s. 181–209, 2022.

[27] C. Kelly, N. Pitropakis, A. Mylonas, S. McKeown ja W. J. Buchanan, ”A Comparative Analysis of Honeypots on Different Cloud Platforms”, *Sensors*, vol. 21, nro 7, s. 2433, huhtikuu 2021.

[28] L. Spitzner, ”Definitions and Value of Honeypots”, 2019. url: `https://api.semanticscholar.org/CorpusID:198957004`.

[29] M. S. Zemene ja P. Avadhani, ”Implementing high interaction honeypot to study SSH attacks”, teoksessa *2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2015, s. 1898–1903. DOI: `10.1109/ICACCI.2015.7275895`.

[30] M. Rabzelj, L. Š. Južnič, M. Volk, A. Kos, M. Kren ja U. Sedlar, ”Designing and evaluating a flexible and scalable HTTP honeypot platform: architecture, implementation, and applications”, *Electronics*, vol. 12, nro 16, s. 3480, 2023.

[31] A. Vetterl ja R. Clayton, ”Bitter harvest: Systematically fingerprinting low-and medium-interaction honeypots at internet scale”, teoksessa *12th USENIX Workshop on Offensive Technologies (WOOT 18)*, 2018.

[32] Y. Alosefer ja O. Rana, ”Honeyware: a web-based low interaction client honeypot”, teoksessa *2010 Third International Conference on Software Testing, Verification, and Validation Workshops*, IEEE, 2010, s. 410–417.

[33] O. Ayeni, B. Alese ja L. Omotosho, ”Design and implementation of a medium interaction honeypot”, *International Journal of Computer Applications*, vol. 70, nro 22, 2013.

[34] X. Qin, F. Jiang, M. Cen ja R. Doss, ”Hybrid cyber defense strategies using HoneyX: A survey”, *Computer Networks*, vol. 230, s. 109 776, heinäkuu 2023.

[35] E. D. Saputro, Y. Purwanto ja M. F. Ruriawan, ”Medium interaction honeypot infrastructure on the internet of things”, teoksessa *2020 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS)*, IEEE, 2021, s. 98–102.

[36] V. Nicomette, M. Kaâniche, E. Alata ja M. Herrb, ”Set-up and deployment of a high-interaction honeypot: experiment and lessons learned”, *Journal in Computer Virology*, vol. 7, nro 2, s. 143–157, kesäkuu 2010.

[37] N. Ilg, P. Duplys, D. Sisejkovic ja M. Menth, ”A survey of contemporary open-source honeypots, frameworks, and tools”, *Journal of Network and Computer Applications*, vol. 220, s. 103 737, marraskuu 2023.

[38] R. R. Krishna, A. Priyadarshini, A. V. Jha, B. Appasani, A. Srinivasulu ja N. Bizon, ”State-of-the-art review on IoT threats and attacks: Taxonomy, challenges and solutions”, *Sustainability*, vol. 13, nro 16, s. 9463, 2021.

[39] P. Killeen, C. Lin, F. Li, I. Kiringa ja T. Yeap, ”IoT-Based Smart Farming Architecture Using Federated Learning: a Nitrous Oxide Emission Prediction Use Case”, *ACM J. Comput. Sustain. Soc.*, 2025. url: https://doi.org/10.1145/3723039.

[40] A. Aziz, ”Industrial IoT, Cyber-Physical Systems, and Digital Twins”, tohtorinväitöskirja, Luleå University of Technology, 2021.

[41] Palo Alto Networks, *2020 Unit 42 IoT Threat Report — unit42.paloaltonetworks.com*, https://unit42.paloaltonetworks.com/iot-threat-report-2020/, (Viitattu 19.3.2025).

[42] NETGEAR Security Team, *The 2024 IoT Security Landscape Report - NETGEAR — netgear.com*, https://www.netgear.com/hub/network/2024-iot-threat-report/, (Viitattu 21.03.2025).

[43] D21DCS151, *A case study on Mirai Botnet Attack of 2016 — d21dcs151*, https://medium.com/@d21dcs151/a-case-study-on-mirai-botnet-attack-of-2016-4b66630e6508, (Viitattu 22.03.2025).

[44] Y. Liu ja H. Wang, ”Tracking mirai variants”, *Virus Bulletin*, s. 1–18, 2018.

[45] Z. Ling, Y. Xu, Y. Jin, C. Zou ja X. Fu, ”New variants of mirai and analysis”, *Encyclopedia of Wireless Networks*, s. 1–8, 2020.

[46] C. Onyagu, O. Okonkwo, G. Akawuku ja J. John, ”Enhancing Security in Internet of Things (IoT) Architecture through Defense-in-Depth Mechanism: A Comprehensive Study”, *NEWPORT INTERNATIONAL JOURNAL OF ENGINEERING AND PHYSICAL SCIENCES*, vol. 4, s. 17–22, maaliskuu 2024. DOI: 10.59298/NIJEP/2024/411722.1.1100.

[47] K. Xu, X. Wang, W. Wei, H. Song ja B. Mao, ”Toward software defined smart home”, *IEEE Communications Magazine*, vol. 54, nro 5, s. 116–122, 2016. DOI: 10.1109/MCOM.2016.7470945.

[48] J. Franco, A. Aris, B. Canberk ja A. S. Uluagac, ”A Survey of Honeypots and Honeynets for Internet of Things, Industrial Internet of Things, and Cyber-Physical Systems”, *IEEE Communications Surveys & Tutorials*, vol. 23, nro 4, s. 2351–2383, 2021. DOI: 10.1109/COMST.2021.3106669.

[49] B. B. Zarpelão, R. S. Miani, C. T. Kawakani ja S. C. de Alvarenga, ”A survey of intrusion detection in Internet of Things”, *Journal of Network and Computer Applications*, vol. 84, s. 25–37, 2017, ISSN: 1084-8045. DOI: https://doi.org/10.1016/j.jnca.2017.02.009.

[50] H. Taşçı, S. Gönen, M. A. Barışkan, G. Karacayılmaz, B. Alhan ja E. N. Yılmaz, ”Password attack analysis over honeypot using machine learning password attack analysis”, *Turkish Journal of Mathematics and Computer Science*, vol. 13, nro 2, s. 388–402, 2021.

[51] P. Lanka, K. Gupta ja C. Varol, ”Intelligent Threat Detection—AI-Driven Analysis of Honeypot Data to Counter Cyber Threats”, *Electronics*, vol. 13, nro 13,

s. 2465, kesäkuu 2024, ISSN: 2079-9292. DOI: 10.3390/electronics13132465. url: http://dx.doi.org/10.3390/electronics13132465.

[52] Allot, *Brute Force Attacks on IoT - Here to Stay? - Allot — allot.com*, https://www.allot.com/blog/brute-force-attacks-iot/, (Viitattu 28.03.2025).

[53] T. Shah ja S. Venkatesan, ”A Method to Secure IoT Devices Against Botnet Attacks”, teoksessa *Internet of Things – ICIOT 2019*. Springer International Publishing, 2019, s. 28–42, ISBN: 9783030233570. DOI: 10.1007/978-3-030-23357-0_3.

[54] P. Celeda, R. Krejci ja V. Krmicek, ”Revealing and analysing modem malware”, teoksessa *2012 IEEE International Conference on Communications (ICC)*, 2012, s. 971–975. DOI: 10.1109/ICC.2012.6364598.

[55] Y. Zhou, ”Chameleon: Towards adaptive honeypot for internet of things”, teoksessa *Proceedings of the ACM Turing Celebration Conference-China*, 2019, s. 1–5.

[56] I. Mokube ja M. Adams, ”Honeypots: concepts, approaches, and challenges”, teoksessa *Proceedings of the 45th Annual ACM Southeast Conference*, sarja ACMSE ’07, Winston-Salem, North Carolina: Association for Computing Machinery, 2007, s. 321–326, ISBN: 9781595936295. DOI: 10.1145/1233341.1233399.

[57] M. T. Qassrawi ja H. Zhang, ”Client honeypots: Approaches and challenges”, teoksessa *4th International Conference on New Trends in Information Science and Service Science*, 2010, s. 19–25.

[58] M. L. Bringer, C. A. Chelmecki ja H. Fujinoki, ”A survey: Recent advances and future trends in honeypot research”, *International Journal of Computer Network and Information Security*, vol. 4, nro 10, s. 63, 2012.

[59] D. Fraunholz, M. Zimmermann ja H. D. Schotten, ”An adaptive honeypot configuration, deployment and maintenance strategy”, teoksessa *2017 19th International*

Conference on Advanced Communication Technology (ICACT), IEEE, 2017, s. 53–57.

[60] N. Nishad ja R. Singh, ”Honeypot deployment: A blockchain-based distributed approach”, *International Journal of Intelligent Communication and Computer Science*, vol. 2, nro 1, s. 72–81, 2024.

[61] C. Lim, M. Marcello, A. Japar, J. Tommy ja I. E. Kho, ”Development of Distributed Honeypot Using Raspberry Pi”, teoksessa *International Conference on Information, Communication Technology and System*, 2014.