Kuluttajille suunnattujen IoT-kameroiden tietoturvahaasteet ja keinoja niiden hallintaan

Turun yliopisto
Tietotekniikan laitos
TkK-tutkielma
Tietotekniikka
Kesäkuu 2025
Aino Aakko

TURUN YLIOPISTO
Tietotekniikan laitos

Aino Aakko: Kuluttajille suunnattujen IoT-kameroiden tietoturvahaasteet ja keinoja niiden hallintaan

TkK-tutkielma, 25 s.
Tietotekniikka
Kesäkuu 2025

IoT-laitteiden suosio on kasvanut kuluttajien keskuudessa kuluttajien rakentaessa älykoteja arjen helpotukseksi. Samalla IoT-kameroiden suosio on kasvanut, sillä niiden avulla on helppo valvoa kotia hallintasovelluksen kautta. Samalla näiden laitteiden tietoturva on myös noussut merkittäväksi huolenaiheeksi.
Tässä tutkielmassa tarkastellaan IoT-kameroiden tietoturvahaasteita kuluttajakäytössä sekä keinoja, joilla näitä haasteita voidaan torjua. Tutkimuksessa analysoidaan IoT-kameroiden yleisimpiä haavoittuvuuksia, kuten oletussalasanojen käyttöä, ohjelmistopäivitysten laiminlyöntiä ja salaamattomia yhteyksiä. Lisäksi käsitellään tunnettuja haittaohjelmia, jotka hyödyntävät näitä haavoittuvuuksia.
Tutkielmassa esitellään suojatoimenpiteitä niin laitevalmistajien kuin kuluttajienkin näkökulmasta, ja tuodaan esiin myös koneoppimisen rooli uhkien torjunnassa. Työn perusteella voidaan todeta, että sekä tekniset ratkaisut että lainsäädännölliset toimet ovat välttämättömiä IoT-kameroiden tietoturvan parantamiseksi. Kuluttajien tietoisuuden lisääminen ja valmistajien vastuun korostaminen ovat keskeisiä tekijöitä turvallisempien IoT-järjestelmien rakentamisessa.

Asiasanat: IoT-kamera, tietoturva, tietoturvahaaste, kuluttaja, suojatoimenpide

Sisällys

Taulukot

1 Johdanto

Esineiden internet (engl. Internet of Things, IoT) on tullut osaksi useimpien ihmisten arkea. IoT-laitteet, kuten älykellot, valvontakamerat ja kodinkoneet helpottavat kuluttajien elämää ja tuottavat tietoa, reaaliaikaista valvontaa sekä ohjausta. Erityisesti kuluttajakäyttöön suunnattujen IoT-kameroiden suosio on kasvanut nopeasti, koska ne mahdollistavat käyttäjälle esimerkiksi omaisuuden tarkkailemisen etänä mobiilisovelluksen kautta. [1] Samalla näiden IoT-kameroiden suosio hyökkäyksien kohteena on kasvanut. Tietoturvaloukkaukset ovat uhka käyttäjien yksityisyydelle, mikä tekee aiheen tarkastelusta ajankohtaista. [2], [3] IoT-laitteiden tietoturva on tekninen ja yhteiskunnallinen kysymys. Kuluttajien tietoisuus erilaisista tietoturvatoimenpiteistä ja valmistajien vastuu ovat keskeisiä tekijöitä tietoturvallisuuden ylläpitämisessä. [4]

Tämä kirjallisuuskatsaus tarkastelee kuluttajakäyttöön tarkoitettujen IoT-kameroiden tietoturvahaasteita. Tämän tutkielman tavoitteena on ymmärtää, millaisia tietoturvariskejä näihin laitteisiin liittyy, millainen vastuu eri toimijoilla on tietoturvan parantamiseksi ja mitä ratkaisuja tai toimintatapoja on esitetty tietoturvan parantamiseksi. Tutkielman tutkimuskysymykset ovat seuraavat:

TK1: *Mitä tietoturvahaasteita on kuluttajakäyttöön suunnatuissa IoT-kameroissa?*

TK2: *Millaisia toimenpiteitä voidaan tehdä IoT-kameroiden tietoturvan parantamiseksi?*

Hakukantana on toiminut pääasiassa IEEE Xplore. Google Scholaria ja Volter-tietokantaa on myös käytetty yksittäisten artikkelien hakemiseen. IEEE Xploressa hakulausekkeena on käytetty: *("cybersecurity" OR "security") AND ("IoT" OR "internet of things") AND ("web*camera*" OR "camera*" OR "IP*camera*")*. Tällä hakulausekkeella hakutuloksia on ollut 2332 kappaletta. Hakua on suodatettu vuosille 2015-2025 ja tällöin hakutuloksia on ollut 2303. Näistä tuloksista artikkeleita on valittu otsikon ja tiivistelmän perusteella. Tutkielman edetessä myös jo valittujen artikkeleiden lähdeluettelosta on haettu lisää lähteitä tähän tutkielmaan.

Kandidaatintutkielman toisessa luvussa ensimmäisenä esitellään yleisluontoisesti, mitä esineiden internetillä eli IoT:llä tarkoitetaan. Lisäksi toisessa luvussa selvennetään millaisia tietoturvavaatimuksia IoT-laitteiden tulisi noudattaa, jotta IoT-laitteiden käyttäjien data ja tiedot olisivat turvassa. Viimeisenä toisessa luvussa kerrotaan myös yleisesti älykotien tietoturvasta. Tutkielman kolmannessa luvussa käsitellään IoT-kameroiden tietoturvahaasteita eli esimerkiksi millaisia haavoittuvuuksia erilaisista IoT-kameroista löytyy. Lisäksi luvussa esitellään vielä erilaisia tunnettuja haittaohjelmia, jotka ovat vaikuttaneet IoT-kameroiden turvallisuuteen. Neljännessä luvussa kerrotaan minkälaisia suojatoimenpiteitä voidaan tehdä erilaisia tietoturvahyökkäyksiä vastaan. Tutkielman viidennessä luvussa käydään läpi tutkielman keskeisimmät havainnot, jotka liittyvät tietoturvauhkiin ja niiden ratkaisuihin. Lopuksi kuudennessa luvussa tiivistetään tutkielman sisältö eli kerrotaan, mitä luvuissa 2-4 käsiteltiin.

2 Esineiden internet ja älykodin tietoturva

2.1 Esineiden internet

IoT-laite on järjestelmä, joka sisältää joko sensoreita tai toimilaitteita tai molempia. Laite tukee Internet-yhteyttä joko suoraan tai jonkin välittäjän kautta. Sensorit mittaavat jotakin osaa maailmasta ja laite päivittää keräämänsä tiedot Internetiin ja pilvipalveluihin. [5] IoT-laitteissa sensoreina voivat muun muassa toimia kamerat, mikrofonit ja liiketunnistimet [2]. Toimilaitteet ovat elektronisesti ohjattuja laitteita, joilla voidaan vaikuttaa ja havainnoida fyysistä maailmaa. Yleisiä IoT-laitteisiin liitettyjä toimilaitteita voivat olla esimerkiksi valot, lukot, moottorit ja releet. Esineiden internet on siis sensorien, toimilaitteiden ja Internet-järjestelmien verkosto. Esimerkiksi verkkosivustot ja pilvipalvelimet ovat Internet-järjestelmiä, jotka ovat yhteensopivia viestimään sensorien ja toimilaitteiden kanssa. [5]

Kuusi suosittua tiedonsiirtoteknologiaa, joita käytetään markkinoilla olevissa IoT-laitteissa ovat Wireless local area network (WLAN), Zigbee, Bluetooth low energy (BLE), IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN), Long Range Wide Area Network (LoRaWAN) ja Radio frequency identification (RFID) [4]. Esimerkiksi kotia automatisoidessa voidaan hyödyntää Zigbeetä. Tällöin kodin sisällä IoT-laitteiden välinen vuorovaikutus tapahtuu Zigbeen luoman mesh-

verkon kautta [6]. IoT-laitteet tukevat yleensä sekä IPv4- (Internet Protocol version 4) ja IPv6-osoitteita (Internet Protocol version 6), mikä takaa niille laajan osoiteavaruuden ja mahdollistaa niiden yhdistämisen laajempaan internetiin. Tämä mahdollistaa niiden etäohjauksen ja valvonnan erilaisissa käyttökohteissa. IoT-laitteet voivat toimia automaattisesti ilman jatkuvaa ihmisen väliintuloa, mutta niitä voidaan myös hallita ja valvoa etänä esimerkiksi älypuhelimen tai tietokoneen välityksellä. [1]

IoT-teknologiaa hyödynnetään laajasti niin kotitalouksissa kuin teollisuuden automatisoiduissa ympäristöissä ja älykaupungeissa, mikä tekee siitä keskeisen osan nykyaikaista digitalisaatiota. [1] Esimerkiksi valvontakameroista voidaan seurata reaaliaikaista videokuvaa tai robotti-imuri voidaan käynnistää imuroimaan etänä. IoT-laitteet ovat siis käteviä erilaisissa automatisoiduissa ympäristöissä.

IoT-laitteet voivat käyttää kommunikaatiossa asiakas-palvelin (engl. client-server) -vuorovaikutusta. Asiakas-palvelin -mallia käytetään, kun tietoja lähetetään käyttäjälle. Käyttäjä pystyy esimerkiksi erillisellä hallintasovelluksella ohjaamaan IoT-laitetta internetin välityksellä mistä tahansa. Palvelin vastaa tiedonsiirrosta käyttäjän mobiililaitteen ja kodin IoT-järjestelmän välillä. [6] IoT-verkkojen arkkitehtuurin voi yleisesti jakaa kolmeen kerrokseen, mitkä ovat sovelluskerros (engl. Application layer), verkkokerros (engl. Network layer) ja fyysinen kerros (engl. Physical layer). IoT-arkkitehtuurissa fyysinen kerros kerää tietoa, verkkokerros siirtää sen, ja sovelluskerros käsittelee ja esittää tiedon käyttäjälle. Käyttäjän vaikutus on suurin sovelluskerroksessa ja vähäisin fyysisessä kerroksessa. Kerrosten toimintaa on kuvattu taulukossa 2.1. [7], [8]

Taulukko 2.1: Esineiden internetin arkkitehtuurikerrokset ja niiden ominaisuudet

Arkkitehtuurikerros	**Pääasiallinen tehtävä**	**Esimerkkiteknologiat ja -laitteet**	**Käyttäjän vuorovaikutus**
Sovelluskerros	Järjestelmän hallinta, tiedon käsittely ja esittäminen	Pilvipalvelut, käyttöliittymät, mobiili- ja web-sovellukset	Suora: käyttäjä näkee ja ohjaa toimintaa
Verkkokerros	Datan siirto laitteiden, verkkojen ja pilvipalveluiden välillä	WLAN, Bluetooth, ZigBee, reitittimet, yhdyskäytävät	Epäsuora: toimii taustalla
Fyysinen kerros	Tiedon keruu ympäristöstä sensorien ja laitteiden avulla	Anturit, RFID, kamera, liiketunnistin	Epäsuora: laitteet toimivat automaattisesti

2.2 IoT-laitteiden tietoturvavaatimuksia

Artikkelissa [4] F. Meneghello ym. esittelee IoT-järjestelmän tietoturvavaatimuksia, jotka jaotellaan kolmeen eri toimintatasoon. Nämä tasot ovat tieto-, käyttöoikeus- ja toimintotaso. Tietotasolla tietoturvan tulee taata järjestelmän eheys, anonymiteetti, luottamuksellisuus ja yksityisyys. Eheys tarkoittaa sitä, että vastaanotettua dataa ei saa olla muutettu lähetyksen aikana. Anonymiteetti taas tarkoittaa sitä, että tietolähteen henkilöllisyyden pitäisi pysyä piilossa kolmansilta osapuolilta. Luottamuksellisuus tarkoittaa sitä, etteivät kolmannet osapuolet pääse lukemaan tietoa. Yksityisyys tarkoittaa, ettei asiakkaan yksityisiä tietoja saa paljastaa tiedonvaihdon aikana ja salakuuntelijoille tunnistettavan tiedon päätteleminen on oltava vaikeaa. [4]

Käyttöoikeustaso määrittää tietoturvamekanismeja, joilla valvotaan verkkoon pääsyä. Tähän tasoon sisältyy käyttöoikeuksien hallintaa, autentikointia ja valtuutuksen varmistamista. Käyttöoikeuksien hallinta takaa sen, että vain lailliset käyttäjät voivat käyttää laitteita ja verkkoa hallinnollisiin tehtäviin. Autentikaatio tarkistaa laitteen oikeuden verkkoon pääsemiseen ja verkon oikeuden yhdistyä kyseiseen

laitteeseen. Autentikointi on todennäköisesti ensimmäinen toiminto, joka suoritetaan uuteen verkkoon liittyessä. Valtuutuksella varmistetaan, että vain valtuutetut laitteet ja käyttäjät saavat pääsyn verkkopalveluihin tai -resursseihin. [4]

Toimintotasolla määritellään tietoturvavaatimukset resilienssin ja itseorganisoitumisen perusteella. Resilienssi viittaa verkon kykyyn taata verkkoon yhdistettyjen laitteiden turvallisuus myös hyökkäysten ja vikojen yhteydessä. Itseorganisoituminen tarkoittaa IoT-järjestelmän kykyä korjata itseään pysyäkseen toimintakykyisenä silloinkin, kun jotkin sen osat eivät toimi satunnaisen toimintahäiriön tai hyökkäysten vuoksi. [4]

2.3 Älykotien tietoturva

Viime vuosina IoT-laitteiden käyttö on yleistynyt kuluttajien keskuudessa. IoT-laitteiden avulla he ovat alkaneet rakentaa itselleen niin kutsuttuja älykoteja. IoT-laitteiden avulla voidaan esimerkiksi suojata kotia käyttämällä valvontakameroita ja liiketunnistimia tai tehdä elämisestä muuten vain mukavampaa automatisoimalla laitteita. Samalla nämä IoT-laitteet kuitenkin tuovat kotiin turvallisuusriskin. IoT-laitteet ovat houkutteleva kohde hakkereille, minkä vuoksi niiden suojaus ja tietoturva on erityisen tärkeää. [2]

IoT-laitteet ovat alttiimpia haitallisille käyttöyrityksille kuin perinteiset verkkoon yhdistämättömät laitteet, koska ne ovat jatkuvasti yhteydessä internetiin ja laitteet kommunikoivat keskenään eri teknologioiden kautta [1]. IoT-kamerat ovat houkutteleva hyökkäyskohde, sillä niitä asennetaan kodeissa usein intiimeihin paikkoihin kuten makuuhuoneeseen tai olohuoneeseen. IoT-kameroita valmistetaan moniin eri tarkoituksiin. Esimerkiksi vauvojen tarkkailuun tarkoitetut itkuhälyttimet ja erilaiset valvontakamerat ovat IoT-kameroita. Näille nettiin yhdistetyille kameroille on ominaista niiden yhdistäminen puhelimeen jonkin hallintasovelluksen kautta. [3]

Verkkoyhteydellä varustetut laitteet on siis tärkeä suojata siten, etteivät ne joudu väärinkäytösten kohteiksi vaarantaen käyttäjien yksityisyyden. IoT-laitteiden määrä ja käyttö kasvaa nopeasti, mutta niiden tietoturva vaatii huomiota erityisesti kodin verkkoympäristössä. Tietoturvan parantamiseksi voidaan käyttää esimerkiksi salausta, palomuureja ja virustentorjuntaohjelmia. IoT-laitteiden suojausteknologioiden kehittämissä haastetta luo laitteiden rajoitettu akkukapasiteetti, hidas prosessointikyky ja pieni muistitila. [1]

Monet kuluttajille suunnatut IoT-laitteet sisältävät haavoittuvuuksia, kuten puutteellista salausta, heikkoa autentikointia ja heikosti suojattuja ohjelmointirajapintoja. Heikosti suojatut IoT-valvontakamerat voivat esimerkiksi mahdollistaa luvattoman pääsyn sen tallentamaan videomateriaaliin rikkoen näin käyttäjän yksityisyyttä. IoT-laitteiden tulisi siis käyttää vahvoja autentikointimekanismeja, kuten monivaiheista tunnistautumista. Tätä voidaan hyödyntää esimerkiksi sovelluksissa, joiden avulla IoT-laitteita käytetään. Lisäksi oletussalasanojen vaihtaminen, palomuurien käyttö ja ohjelmistopäivityksien ajantasaisuus vaikuttavat kodin tietoturvaan positiivisesti. [9]

3 IoT-kameroiden tietoturvahaasteet

3.1 Yleiskatsaus tietoturvariskeihin

IoT-laitteisiin liittyy useita tietoturvariskejä, joita käyttäjän on usein vaikea havaita tai hallita itse. Yhtenä ongelmana IoT-laitteissa on se, että laitteet ovat usein samankaltaisia tai identtisiä. Jos hyökkääjä on löytänyt haavoittuvuuden yhdestä laitteesta, voidaan samaa menetelmää hyödyntää myös muihin samankaltaisiin laitteisiin murtautumiseen. Yksittäinen tietoturva-aukko voi siis johtaa laajaan ongelmaan. Laitteen käyttäjä voi myös luulla, että laite toimii normaalisti, vaikka oikeasti laite olisi kaapattu ja se luovuttaisi tietoa ilman lupaa. [1] Hyökkääjä voi murtautuessaan kodin verkkoon ohjata kyseiseen verkkoon liitettyjä järjestelmiä etänä. Tämä mahdollistaa hyökkääjälle pääsyn esimerkiksi valvontakameran tietoihin. [2] Tällöin hyökkääjällä on pääsy arkaluontoiseen ja yksityiseen videomateriaaliin uhrin ympäristöstä [4]. Näiden tietojen avulla hyökkääjä voi esimerkiksi selvittää, onko talossa ihmisiä. Tätä tietoa voidaan käyttää hyväksi, jos esimerkiksi taloon suunnitellaan murtautumista. [2]

IoT-laitteiden tietoturvaongelmia aiheuttaa jo se, että laitteiden valmistuvaiheessa valmistajat eivät panosta tarpeeksi laitteiden tietoturvaan. Tietoturvallisuus tulisi ottaa huomioon jo uusien laitteiden suunnitteluvaiheessa eli valmistajien ja suunniteloijen tulisi käyttää Security by design -periaatetta. Laitteista pitäisi suunnittella sellaisia, että niissä on helpompi ottaa käyttöön tietoturvaa parantavia teknologioi-

ta. IoT-laitteiden energia-, viestintä-, laskenta- ja tallennuskapasiteetit ovat todella rajallisia, mikä vaikeuttaa entisestään turvamekanismien käyttöönottoa. IoT-laitteet kaipaavat siis uudenlaisia ratkaisuja tietoturvan käytössä. Myöskään IoT-laitteiden valmistajilla ei välttämättä ole asiantuntemusta kyberturvallisuudesta tai tietoturvariskeistä, joita syntyy, kun laitteita liitetään internetiin. Laitevalmistajen lisäksi laitteiden loppukäyttäjillä ei myöskään välttämättä ole tietoa tietoturvakäytännöistä. Loppukäyttäjät eivät usein toteuta edes kaikkein yksinkertaisinta tietoturvakäytäntöä laitteeensa suojaksi eli laitteen oletussalasanan muuttamista ensimmäisellä käyttökerralla. [4]

3.2 Yleiset haavoittuvuudet

Kodin IoT-järjestelmä koostuu yleensä IoT-laitteesta, hallintasovelluksesta ja pilvipalvelusta, jossa dataa säilytetään. Eli IoT-laitteiden riskit eivät liity pelkästään itse laitteeseen vaan myös käytössä olevaan sovellukseen ja pilvipalveluun. [10] IoT-kameroiden hyökkäys voi siis tulla sisältä tai ulkoa. Yleensä hyökkäykset tapahtuvat niin sanotusti sisäisesti jossakin pilvipalvelussa tai palvelimella. Yleensä tällöin näistä paikoista saadaan kerättyä käyttäjien henkilökohtaista dataa. [5] IoT-arkkitehtuurissa sovelluskerros käsittelee älylaitteita ja antureita, jotka suorittavat erilaisia tehtäviä. Sovelluskerros myös ohjaa järjestelmää ja näyttää IoT-laitteiden keräämää dataa. On siis tärkeää, että hallintasovelluksissa ja pilvipalveluissa ei ole esimerkiksi ohjelmisto tai laitevikoja tietoturvallisuuden takaamiseksi. [7]

Kameroihin fyysisesti ulkoapäin kohdistuvat hyökkäykset johtuvat usein siitä, että kameroita ei ole voitu asentaa turvalliseen paikkaan, missä ainoastaan käyttäjä voisi käsitellä kameraa. Tämä mahdollistaa hyökkääjälle kameroiden ulkoisen manipuloinnin. Fyysiset hyökkäykset ovat yleisiä ja monimuotoisia. Osassa IoT-kameroista on sisäinen tallennus, jolloin kamerassa käytetään SD-muistikorttia (engl. Secure Digital card) sisällön varmuuskopiointiin. Tällainen kamera mahdollistaa ri-

kollisten pääsevän fyysisesti käsiksi kameraan ja henkilökohtaisiin tietoihin. Useimmat IoT-kamerat kuitenkin käyttävät pilvipalveluihin tallentamista. Hyökkääjät pystyvät manipuloimaan solmuja (engl. nodes) joihin tietoja siirretään ja täten saamaan pääsyn käyttäjän tietoihin. Hyökkääjät pystyvät häiritsemään myös esimerkiksi kameroiden RFID-tunnisteiden toimintaa manipuloimalla radiotaajuutta ja tällöin samalla vaikeuttaa tiedonsiirtoa. Tämä on yksi muoto Denial of Service (DoS) hyökkäyksestä eli palvelunestohyökkäyksestä. [3]

Yleensä IoT-laitteita käytetään puhelimella jonkin hallintasovelluksen kautta langattoman yhteyden välityksellä. Hallintasovellus vaatii usein käyttäjätunnuksen luonnin ja tähän liittyy usein myös omien tietojen syöttämistä sovellukseen. Sovellukseen rekisteröitymisen jälkeen IoT-laitteet ovat yhteydessä sovellukseen ja IoT-laitteet alkavat keräämään tietoa, jota voidaan näyttää sovelluksessa käyttäjälle. Nämä käyttäjien syöttämät tiedot ja IoT-laitteen keräämät tiedot saattavat vuotaa sovelluksista erilaisten ohjelmistovikojen ja puutteiden takia. [10]

IoT-laitteiden hyödyntämistä ohjelmistoista löytyvät haavoittuvuudet julkaistaan Common Vulnerabilities and Exposures (CVE) -tietokannassa ja uusien haavoittuvuuksien ilmaantuessa jotkut laitevalmistajat myös julkaisevat IoT-laitteelleen uuden ohjelmistopäivityksen. Useat IoT-laitteiden käyttäjät eivät kuitenkaan ole tietoisia mahdollisista haavoittuvuuksista. Käyttäjät usein asentavat laitteen eivätkä sen jälkeen päivitä IoT-laitteiden ohjelmistoa tai sitten he tekevät sen todella harvoin. Laitteisiin hyökkäyksiä tekevät hakkerit hyödyntävät käyttäjien epätietoisuutta tekemällä hyökkäyksiä päivittämättömiin IoT-laitteisiin. [11]

Yleensä ohjelmistotaso on hyvä lähtökohta IoT-laitteen haavoittuvuuksien hyödyntämiselle. IoT-laitteita hallitaan usein esimerkiksi mobiilisovelluksen tai selainpohjaisen käyttöliittymän avulla. Näitä käyttöliittymiä voidaan yrittää käyttää laitteen luvattomaan hallintaan. Luvaton hallinta on helppoa, jos laite ei vaadi mitään kirjautumista sovelluksessa. Myöskin erilaiset käyttäjänimet ja salasanat voi olla

helppo selvittää, jos sovellus tallentaa käyttäjän kirjautumistiedot johonkin tietokantaan. Tietokannassa käyttäjänimi voi tallentua selväkielisenä, mikä tarkoittaa ettei käyttäjänimeä ole yritettu suojata millään tavalla. Myös salasana saatetaan tallentaa tietokantaan vanhentuneilla suojausmenetelmillä, jotka ovat helposti murrettavissa erilaisilla salasananmurtotyökaluilla. [12]

Esimerkiksi kyberfyysisissä hyökkäyksissä hyödynnetään laitteen fyysisiä komponentteja, kuten antureita, joihin vaikuttamalla hyökkääjä voi saada pääsyn järjestelmään tai sen tietoihin. Tällaiset hyökkäykset voivat luoda järjestelmään piilotettuja takaovia, joita on vaikea havaita. Ohjelmistohyökkäykset taas perustuvat haittaohjelmien asentamiseen laitteisiin. Tällöin hyökkääjä pystyy varastamaan tai tuhoamaan tietoa. Jos laitteen käyttäjätunnukset päätyvät hyökkääjän käsiin, koko laitteen hallinta voi siirtyä hyökkääjälle. Verkon kautta tehtävät hyökkäykset ovat myös yleisiä ja palvelunestohyökkäykset ovat yksi esimerkki tällaisesta. Palvelunestohyökkäyksessä suuri määrä kaapattuja IoT-laitteita toimii yhdessä ja kuormittaa kohdejärjestelmää niin, että kohdejärjestelmä lakkaa toimimasta. Näissä hyökkäyksissä käytetään usein yhtä keskitettyä komentopalvelinta, joka hallitsee bottiverkkoa. [13]

Vuonna 2003 CCTV Calculator nettisivustolla [14] on julkaistu haavoittuvuuslista, jossa ilmoitetaan tunnettuja haavoittuvuuksia suljetuissa kameravalvontajärjestelmissä (engl. Closed-circuit television cameras, CCTV cameras). Listaa on vuoden 2003 jälkeen päivitetty uusien haavoittuvuuksien tullessa ilmi. Viimeksi listaa on päivitetty vuonna 2024. IoT-laitteiden tietoturva on ollut keskeinen globaali huolenaihe erityisesti vuodesta 2016 lähtien, jolloin Mirai-haittaohjelman bottiverkko hyödynsi haavoittuvaisia IoT-laitteita. Tämän seurauksena vuonna 2017 haavoittuvuuslistassa oli mukana monia tunnettuja IoT-kameroiden valmistajia, kuten Samsung, Hikvision, Kguard, AirLink, Genivia, TP-Link, Foscam, Panasonic, D-link ja

Sony. Muutamia IoT-kameroiden haavoittuuksia vuonna 2017 kuvataan taulukossa 3.1.

Taulukko 3.1: Esimerkkejä IoT-laitteiden tietoturvahaavoittuvuuksista vuonna 2017

Laitemalli tai ohjelmisto	**Haavoittuvuuden tyyppi**	**Vaikutus tai uhka**	**Hyökkäystapa tai reitti**
Samsung NVR	MD5-salasanatiivisteen paljastuminen	Mahdollistaa kirjautumisen admin-tunnuksella	JSON-pyynnön kautta
Hikvision iVMS-4200 (v.<2.6.2.7)	Salasanan palautuskoodien generointi	Paikallinen käyttäjä voi murtaa käyttöoikeuksia	Paikallinen pääsy
Kguard DVR 104/108 v2	Ei todennusta tai valtuutusta	Kuka tahansa voi käyttää laitetta	ActiveX-yhteys ilman rajoitteita
AirLink101 SkyIPCam1620W	Komento-injektio (shell)	Etäkomentojen suoritus käyttöjärjestelmään	CGI-parametrin väärinkäyttö
Genivia gSOAP (v.<2.8.48)	Puskuriylivuoto XML-tiedostossa	Palvelunesto tai mielivaltainen koodi	Suuri XML-dokumentti
TP-Link NC250 (v. 1.2.1)	Ei todennusta videolle	Kuka tahansa voi katsoa videokuvaa	rtsp://-osoitteen kautta
Foscam C1 (v. 2.52.2.37)	HTTP-puskuriylivuoto	Sovelluksen kaatuminen tai muu häiriö	Muotoiltu HTTP-pyyntö
Foscam C1 (v. 2.52.2.37)	Merkkien injektointi salasanan vaihdossa	Chroot-rajoitusten ohitus	HTTP-pyyntö käyttäjänimen vaihdolla
Foscam C1 (v. 2.52.2.37)	Shell-merkkejä NTP-asetuksissa	Komento-injektio laitteen komentotilaan	HTTP-pyyntö NTP-konfiguraatiossa
Foscam C1 (v. 2.52.2.37)	Shell-merkkejä verkkoasetuksissa	Komento-injektio mahdollinen	HTTP-pyyntö verkkoasetuksissa

Tätä tunnettujen haavoittuvuuksien listaa on päivitetty viimeksi vuonna 2024, jolloin haavoittuvuuksia on esiintynyt esimerkiksi D-Linkin ja Univiewin IoT-kameroissa. D-linkin DCS-8300LHV2 -mallin kamerassa haavoituuvuus liittyy kovakoodattuun PIN-tunnistukseen. Tämä siis mahdollistaa todennuksen ilman salasanaa eli hyökkääjä voi päästä suoraan laitteen hallintaan ilman valtuuksia. Hyökkäys voidaan suorittaa ilman kirjautumista. Univiewin NVR301-04S2-P4 -mallin kamerassa löydetty haavoittuvuus mahdollistaa reflektio-XXS-hyökkäyksen (engl. reflected cross-site scripting, XXS). Hyökkäyksessä hyökkääjä voi lähettää käyttäjälle URL-osoitteen, jonka klikkaaminen johtaa haitallisen JavaScript-koodin suorittamiseen käyttäjän selaimessa. Hyökkäyksen toteuttaminen edellyttää kuitenkin ensin kirjautumista laitteeseen, mikä rajaa hieman hyökkäyksen vaikutusaluetta. [14]

3.3 Tunnettuja haittaohjelmia

Vuonna 2016 Mirai-haittaohjelma rakensi bottiverkon hyökkäämällä tuhansiin laitteisiin, joista osa oli IoT-kameroita. [15] Bottiverkkoa hyödynnettiin esimerkiksi palvelunestohyökkäysten tekemisessä. Mirai-haittaohjelma etsii jatkuvasti internetistä laitteita, joihin se voi murtautua. Tämä tapahtuu skannaamalla Internet Protocol (IP)-osoitealueita ja palveluportteja. Löydettyään laitteen, Mirai yrittää kirjautua laitteeseen sisään käyttämällä oletuskäyttäjätunnuksia ja -salasanoja. Laite kaapataan, jos kirjautuminen onnistuu. Tällöin laite liitetään myös osaksi hyökkääjän hallitsemaa kaapattujen laitteiden verkostoa eli bottiverkkoa. Tämä prosessi jatkuu ja aina uuden laitteen kaappaamisen jälkeen laitteen IP-osoite ja kirjautumistiedot ilmoitetaan erilliselle raportointipalvelimelle. Tämän jälkeen hyökkäyksen kohteena olevalle laitteelle ladataan itse haittaohjelma ja uhrilaite alkaa myös etsimään ja tartuttamaan muita laitteita. Bottiverkko-hyökkäyksessä komentopalvelin antaa infektoiduille laitteille pyynnön hyökätä. Mirai toimii komenna ja hallinnoi (engl. Command and Control, CnC) periaatteella eli hyökkääjä on kerännyt itselleen bot-

tiverkon ja hän voi antaa antaa bottiverkolle komentoja etänä sekä hallita näitä kaapattuja laitteita palvelimen välityksellä. [16]

Mirain lähdekoodi on myös vuotanut julkiseksi, minkä takia kuka tahansa voi muunnella koodia ja suorittaa hyökkäyksiä koodin avulla. Vuosien 2016-2017 välillä IoT-verkkohyökkäykset kasvoivat jopa 600 prosenttia ja suuri osa tästä kasvusta on Mirai-haittaohjelmasta johtuvaa. Mirain lisäksi on muitakin haittaohjelmia, kuten QBOT, UPX ja Zollard. QBOT-haittaohjelman toimintaperiaate on samankaltainen kuin Mirain, mutta se ei ole yhtä kehittynyt. UPX on ohjelmointityökalu, joka pakkaa ohjelmia ja se vaikeuttaa haittaohjelmien tutkimista. Zollard-haittaohjelma on mato (engl. worm), joka hyödyntää uhrin laitteen resursseja kryptovaluutan louhintaan käyttäjän sitä itse huomaamatta. [13]

C. Kelly ym. testasi Mirai-haittaohjelman vaikutuksia IoT-laitteisiin ja arvioi eri suojatoimenpiteiden tehokkuutta artikkelissa [13]. Kokeilu jaettiin neljään vaiheeseen. Ensimmäisessä vaiheessa valmisteltiin testiverkko ja konfiguroitiin IoT-kamerat virtuaalikoneympäristössä. Toisessa vaiheessa asennettiin ja käynnistettiin Mirai-haittaohjelma, joka saastutti laitteet bottiverkkohyökkäystä simuloiden. Kolmannessa vaiheessa analysoitiin hyökkäyksen jälkeiset haavoittuvuudet ja kehitettiin suojausratkaisuja niiden torjumiseksi. Neljännessä vaiheessa hyökkäys toistettiin, mutta tällä kertaa suojatut laitteet olivat hyökkäyksen kohteena ja samalla pystyttiin arvioimaan suojaustoimien tehokkuutta. Tutkimuksessa käytettiin kolmea kuluttaja IoT-laitetta, joista kaksi olivat IoT-kameroita ja yhtä virtuaalista simulaatiolaitetta. Simuloitu laite rakennettiin käyttämällä VMware-virtuaalikonetta eristetyssä ja yksityisessä verkossa. Lisäksi virtuaalikoneeseen asennettiin Ubuntu-käyttöjärjestelmä ja Busybox-ohjelmisto. IoT-kamerat olivat Coolead IP Camera ja Sricam IP Camera. Coolead-kamerassa havaittiin avoinna portit Telnet 23, HTTP 80 ja Asterix 8600. Kameraan pääsi käsiksi selaimella portin 80 kautta, mutta Telnet-yhteys avattiin murtautumalla sanakirja-hyökkäyksellä (engl. Dictionary attack), joka hyödyn-

tää oletustunnuksia. Tunnistautumisen jälkeen selvisi, että laitteeseen oli asennettuna haavoittuvainen BusyBox-ohjelmistoversio, joka mahdollisti pääsyn koko tiedostojärjestelmään. Tämä teki laitteesta erityisen alttiin Mirai-haittaohjelmalle ja laitteeseen murtauduttiin yhdeksässä sekunnissa.

Sricam-kamera puolestaan käytti lähinnä mobiilisovellusta eikä tarjonnut web- tai Telnet-palvelinta. Porttiskannaus (engl. Network mapper, Nmap)-skannaus paljasti avoimeksi vain portit 554 ja 5000. Portti 554 käyttää Microsoftin Real time streaming -protokollaa (RTSP), jota hyödynnetään videokuvan striimaamiseen. Tämän protokollan haavoittuvuus mahdollisti Uniform Resource Locator (URL) väsytyshyökkäyksen (engl. brute force attack), jossa kameran suoratoistokanava löytyi ilman tunnistautumista. VideoLan Client (VLC)-mediasoittimella videokuva saatiin näkymään syöttämällä oikea URL-osoite ilman salasanaa. Tämä osoittaa vakavaa puutetta laitteen tietoturvassa. Sricam-kamera osoittautui kuitenkin hyvin suojatuksi laitteeksi haittaohjelmien hyödyntämisen näkökulmasta. Kamera vuosi videokuvaa, mutta kamerassa ei ollut sellaisia portteja avoinna, mitä esimerkiksi Mirai-haittaohjelma olisi voinut käyttää komentojen suorittamiseen. Sricam käytti rajattua määrää välttämättömiä portteja sovelluksen toimintaan, mikä tekee siitä vähemmän alttiin hyökkäyksille. Laitetta ei myöskään saatu kaapattua testissä.

4 IoT-kameroihin kohdistuvilta tietoturvahyökkäyksiltä suojautuminen

4.1 Lainsäädäntö

Euroopan unioni (EU) on ottanut käyttöön yleisen tietosuoja-asetuksen (General Data Protection Regulation, GDPR) vuonna 2016 ja sitä on alettu soveltamaan EU:n jäsenmaissa vuonna 2018. Tämän asetuksen tarkoituksena suojata esimerkiksi erilaisten sovellusten käyttäjien henkilökohtaisia tietoja. Yritysten ja internetpalvelujen tarjoajien siis täytyy pitää huoli riittävästä tietosuojasta ja, että henkilötietoja käytetään turvallisesti. [17]

Vuonna 2019 EU on myös säätänyt asetuksen 2019/881 tieto- ja viestintätekniikan kyberturvallisuussertifioinnista. Euroopan unionin kyberturvallisuusvirastolle (engl. the European Union Agency for Cybersecurity, ENISA) on asetettu tavoitteita ja tehtäviä liittyen Eurooppalaisten kyberturvallisuuden sertifiointijärjestelmään. EU:n kyberturvallisuus sertifiointi auttaa tuotteiden ja palveluiden tarjoajia osoittamaan, että heidän ratkaisunsa ovat turvallisia. Tavoitteena on myös luoda yhteinen tapa mitata ja tunnistaa kyberturvallisuutta EU:n alueella. Sertifiointi on toistaisek-

si vapaaehtoista yrityksille, mutta tulevaisuudessa siitä voi tulla pakollista ainakin joissain tapauksissa. [18]

Myös NIS2 on EU:n kyberturvallisuusdirektiivi, jonka tarkoituksena on parantaa kyberturvallisuutta EU:ssa luomalla yhteinen ja korkea turvataso verkko- ja tietojärjestelmille. Direktiivi velvoittaa yrityksiä ottamaan käyttöön vahvempia riskienhallintatoimia, raportoimaan tietoturvaloukkauksista ja noudattamaan kyberturvallisuuden vähimmäisvaatimuksia. Direktiivi edellyttää myös yritysten varautuvan monenlaisiin uhkiin varmistaakseen toimintansa kokonaisvaltaisen suojan ja toimintakyvyn uhkatilanteissa. Tällaisia uhkia voivat olla kyberhyökkäykset ja fyysiset häiriötilat. Viranomaiset voivat valvoa yrityksiä tarkemmin ja määrätä niille sakkoja, jos vaatimuksia ei noudateta. [19]

4.2 Suojatoimenpiteitä valmistajille

Kuluttajien tietoturva on vahvasti sidoksissa käytettyihin hallintasovelluksiin ja pilvipalveluihin. On tärkeää, että kuluttaja käyttää vain luotettavia hallintasovelluksia ja pilvipalveluja ohjeistetulla tavalla, jotta tietoturvallisuus voidaan taata. Sovellusten ja pilvipalveluiden kehittäjien täytyy olla tietoisia turvallisuusaukoista ja erilaisista haittaohjelmista, jotta kuluttajat voivat olla varmoja käyttämiensä sovellusten ja pilvipalvelujen turvallisuudesta. Sovelluskehittäjien täytyy käyttää sovelluksissa vain vahvoja salausmenetelmiä tietojen suojaamiseksi. [7]

Open Web Application Security Project (OWASP) on kansainvälinen voittoa tavoittelematon järjestö, joka keskittyy verkkosovellusten tietoturvan parantamiseen. OWASP:in keskeinen periaate on, että kaikki heidän tuottamansa materiaali on vapaasti saatavilla. Materiaaliin kuuluu esimerkiksi dokumentaatioita, työkaluja, videoita ja keskustelufoorumeita. OWASP tarjoaa useita työkaluja sovellusten ja pilvipalveluiden tietoturvan arviointiin. Kuka tahansa pystyy siis hyödyntämään materiaaleja sovelluksien tietoturvallisuuden kehittämiseen. OWASP:n tun-

neituin julkaisu on OWASP Top 10 -lista, jota päivitetään säännöllisesti. Lista esittelee kymmenen merkittävintä web-sovellusten tietoturvariskiä. Kansainväliset tietoturva-asiantuntijat ovat koonneet listan ja OWASP suosittelee organisaatioita hyödyntämään listaa heidän toiminnassaan tietoturvariskien hallitsemiseksi. [7]

IoT-laitteiden valmistajat tekevät tietoturvatestauksia ennen kuin laitteet päätyvät kuluttajille. Olisi kuitenkin vielä parempi, jos käyttäjät voisivat myös itse tarkistaa omien IoT-laitteidensa turvallisuuden. Ongelmana kuitenkin on, että suurin osa nykyisistä testausohjelmista toimii vain tietokoneilla ja vaatii teknistä osaamista sekä erillisten ohjelmistojen asentamista. Tällaiset työkalut eivät siis ole käytännöllisiä tavallisille käyttäjille. Itse IoT-laitteiden lisäksi olisi tärkeää tarkistaa myös käytettyjen verkkojen ja hallintasovellusten turvallisuus, joissa saattaa olla haavoittuvuuksia. [11]

Artikkelissa [13] löydettyjen haavoittuvuuksien perusteella C. Kelly ym. ehdottivat seuraavanlaisia vastatoimenpiteitä Mirai-haittaohjelmalle. Esimerkiksi Coolead IP Camera käytössä oleva Telnet 23 -portti oli turvaamaton, koska se lähetti kirjautumistietoja salaamattomana. Telnetin sijasta kannattaisi käyttää esimerkiksi Secure Shelliä (SSH), joka on turvallisempi vaihtoehto. Jotkut uudet haittaohjelmat voivat pystyä hyökkäämään myös SSH:n kautta, mutta se on huomattavasti vaikeampaa sillä SSH käyttää vahvoja tunnistetietoja, joiden ansioista hyökkäyksen tekeminen on vaikeaa sekä aikaa vievää. Kaikissa tilanteissa Telnetin vaihtaminen on hankalaa, koska esimerkiksi Coolead-kamerassa käytössä ollut BusyBox-ohjelmisto ei tue SSH:n käyttöä ilman järjestelmän uudelleen kääntämistä. Jos Telnetiä ei voi poistaa käytöstä, porttinumeron voi muuttaa joksikin toiseksi, koska suurin osa haittaohjelmista etsii usein pelkästään oletusporttia 23.

Coolead-kamera käytti myös Hypertext Transfer Protocol (HTTP)-yhteyttä portissa 80. Vastatoimenpide tälle olisi käyttää HTTP:n sijasta Hypertext Transfer Protocol Secure (HTTPS)-yhteyttä, joka käyttää porttia 443. HTTPS muodostaa sa-

latun ja suojatun yhteyden Secure sockets layer (SSL)-sertifikaattien tai Transport Layer Security (TLS) avulla ja nämä estävät luvattomia osapuolia näkemästä siirrettyä tietoa. TLS on uudempi teknologia, joten sen käyttö on suositeltavampaa. [13]

IoT-kamerat käyttävät usein hallintasovelluksia, joiden kautta käyttäjien on helppo katsoa kameroiden kuvaamaa live-kuvaa älypuhelimesta. Joidenkin sovelluksien ominaisuuksiin saattaa kuulua sähköposti-ilmoitusten lähettäminen käyttäjän sähköpostiosoitteeseen Simple Mail Transfer Protocol (SMTP) avulla esimerkiksi liiketunnistimien aktoivoituessa. SMTP kannattaa poistaa käytöstä, koska sen käyttö voi johtaa sähköpostiosoitteen vuotamiseen ja samalla sähköpostiosoitteen päätymisen roskapostilistalle. Tämä voi johtaa roskapostin saamiseen, sähköpostihuijauksiin ja tietojenkalasteluhyökkäyksiin. Myös File Transfer Protocol (FTP) ja Trivial File Transfer Protocol (TFTP) ovat turvallisuusriski ja ne kannattaa poistaa käytöstä, koska ne mahdollistavat haitallisten tiedostojen siirron laitteelle.

Koneoppimista ja syväoppimista käytetään tietoturvallisuuden parantamisessa esimerkiksi tunkeutumisten havaitsemisessa, koska nämä menetelmät osaavat käsitellä reaaliaikaisia tilanteita ja ne oppivat aiemmista tiedoista. Tällaiset mallit kykenevät tunnistamaan poikkeavaa käyttäytymistä järjestelmässä ja parantamaan sen suojaa. Useita koneoppimisen tekniikoita voidaan käyttää estämään hyökkäyksiä IoT-arkkitehtuurin eri tasoilla. Tällaisia tekniikoita ovat esimerkiksi päätöspuut, neuroverkot ja tukivektorit. [8]

IoT-arkkitehtuurissa sovelluskerroksen hyökkäysten torjumisessa voidaan käyttää esimerkiksi lineaarista tukivektorikonetta (engl. Support vector machine, SVM) haittaohjelmien tunnistamiseen Android-laitteissa. [20] Verkkokerroksen hyökkäyksiin voidaan käyttää esimerkiksi syväuskomusverkkoa (engl. Deep belief network, DBN), joka havaitsee erilaisia hyökkäystyyppejä, kuten palvelunestohyökkäyksiä. Syväuskomusverkoilla toteutetuilla turvamekanismeilla on saavutettu jopa 97 pro-

sentin tunnistustarkkuus. [21] Fyysisen kerroksen hyökkäyksien torjuntakeinona voidaan käyttää järjestelmää, joka toimii esimerkiksi häirintähyökkäyksiä (engl. jamming attack) vastaan. Tässä laite säätää suojaustaan dynaamisesti ilman tietoa hyökkääjästä. Tämä perustuu siihen, että laite mukauttaa suojastasoaan reaaliajassa saavutetun tiedonsiirtonopeuden perusteella. [22]

4.3 Suojatoimenpiteitä kuluttajille

Myös kuluttajilla on mahdollisuus vaikuttaa IoT-kameroidensa turvallisuuteen. Fyysisten hyökkäysten estämiseksi kamerat olisi hyvä asentaa turvallisiin paikkoihin, joihin ulkopuoliset eivät pääse käsiksi. Tärkein toimenpide, minkä kuluttaja voi tehdä turvatakseen IoT-kameroitansa on oletussalasanan vaihtaminen johonkin vahvempaan ja vaikeasti arvattavaan salasanaan. Tällainen toimenpide voi ehkäistä merkittävästi hyökkäyksiä, joissa testataan läpi kaikki oletussalasanat ja yleiset salasanat. [3] IoT-laitteiden käyttäjien olisi myös tärkeää päivittää laitteidensa ohjelmistot heti uusien päivitysten tullessa [11]. Uusia laitteita hankittaessa kuluttajan olisi hyvä harkita laitteita, joilla on esimerkiksi EU:n kyberturvallisuussertifiointi. [18].

Artikkelissa [11] Visoottiviseth V. ym. esittelee mobiilisovellusta nimeltä Mobile Application for Security Assessment towards IoT Devices (MASai), jonka avulla IoT-laitteiden käyttäjät pystyvät itse testaamaan IoT-laitteiden ja niihin liittyvien sovellusten tietoturvaa. Sovellus on suunniteltu Android-laitteille, sillä se on yleisin käyttöjärjestelmä puhelimissa. MASai koostuu kolmesta osasta eli MASai-sovelluksesta, MASai-palvelimesta ja Raspberry Pi pohjaisesta MASai-testilaitteesta. Tämän MASai-mobiilisovelluksen kautta IoT-laitteille voi suorittaa tunkeutumistestejä (engl. penetration testing). MASai-mobiilisovellus toimii yhdessä Raspberry Pi pohjaisen testilaitteen kanssa, jolla varsinainen tunkeutumistestaus tehdään. MASai-palvelin taas mahdollistaa Android-sovellusten syvällisemmän koodin analysoinnin.

5 Pohdinta

Tässä kandidaatintutkielmassa tarkasteltiin kuluttajille suunnattujen IoT-kameroiden tietoturvahaasteita, niihin liittyviä uhkia sekä mahdollisia ratkaisuja. Tutkielmassa kävi ilmi, että IoT-laitteiden nopea yleistyminen on jättänyt tietoturvan kehityksen taka-alalle jättäen monet IoT-laitteet alttiiksi erilaisille tietoturvauhille ja hyökkäyksille. IoT-kamerat keräävät ja välittävät esimerkiksi kodeissa yksityistä videokuvaa ja ääntä, minkä johdosta laitteen puutteellinen tietoturva voi johtaa äärimmäisiin yksityisyydensuojan loukkauksiin.

Merkittävimmät kuluttajille suunnattujen IoT-laitteiden tietoturvahaasteet liittyvät päivitysten puutteeseen, oletussalasanojen käyttöön, haavoittuvuuksiin ohjelmistoissa, päivittämättömiin ohjelmistoihin, salaamattomaan tiedonsiirtoon ja valmistajien välinpitämättömyyteen tietoturvasta. Kuluttajien tietoisuus erilaisista riskeistä on usein alhainen eikä valmistajilla ole laitteiden suuren kysynnän vuoksi motivaatiota kehittää tietoturvaa riittävälle tasolle.

Jos lainsäädäntö ei velvoita valmistajaa kehittämään laitteita tietoturvallisemmiksi, eivät yritykset todennäköisesti ole motivoituneita varmistamaan tuotteidensa tietoturvallisuutta, sillä se aiheuttaa lisää kustannuksia. Lisäksi varsinainen haitta tietoturvapuutteista kohdistuu laitteen käyttäjään eikä laitteen valmistajalle. Valmistajien olisi kuitenkin hyvä muistaa, että kuluttajat haluavat todennäköisesti ostaa sellaisen IoT-kameran, jolla on hyvä maine.

Ratkaisuna tietoturvahaasteisiin IoT-kameroiden valmistajia täytyy velvoittaa parempiin tietoturvakäytäntöihin, kuten päivitysten ajantasaisuuteen ja turvallisiin oletusasetuksiin. Valmistajia voitaisiin myös velvoittaa antamaan kuluttajille selkeät ja hyvät tietoturvaan liittyvät ohjeistukset, joka esimerkiksi ohjaisivat kuluttajaa vaihtamaan oletussalasanan vahvaan salasanaan. Ohjeistuksessa voitaisiin myös kertoa tietoturvariskeistä, joita voi aiheutua ohjeiden noudattamatta jättämisellä. Myös ylipäätänsä kuluttajien tietoisuuden kasvattaminen ja lainsäädännön kehittäminen ovat keskeisiä keinoja ongelmien vähentämiseksi. Vaikka valmistajilla on suuri vastuu turvallisten laitteiden suunnittelussa, myös kuluttajilla ja lainsäätäjillä on tärkeä rooli. Esimerkiksi EU:n GDPR asetuksen myötä EU:n alueella kuluttaja voi luottaa siihen, että yritysten on tallennettava kuluttajien henkilökohtaisia tietoja tietoturvallisilla ja ajantasaisilla menetelmillä.

6 Yhteenveto

Luvussa 2 tarkasteltiin esineiden internetin (IoT) toimintaperiaatteita ja siihen liittyviä tietoturvakysymyksiä erityisesti kuluttajakäyttöön suunnattujen laitteiden näkökulmasta. Luvussa kuvataan, mitä IoT-laitteet ovat ja mikä on niiden toimintaperiaate. Luvussa esitellään myös IoT-verkon kolme arkkitehtuuri kerrosta. Lisäksi luvussa tarkastellaan myös IoT-järjestelmien tietoturvavaatimuksia kolmella eri tasolla, jotka ovat tietotaso, käyttöoikeustaso sekä toimintotaso. Nämä vaatimukset muodostavat perustan IoT-laitteiden turvalliselle käytölle. Lopuksi luvussa 2 käsiteltiin älykotien tietoturvahaasteita. Kuluttajakäyttöön tarkoitetut IoT-laitteet voivat sisältää merkittäviä haavoittuvuuksia ja tietoturvan laiminlyönti voi johtaa vakaviin yksityisyyden loukkauksiin.

Luvussa 3 käsitellään IoT-kameroiden keskeisiä tietoturvahaasteita ja niiden vaikutusta kuluttajakäyttöön. Lisäksi luku 3 käsitteli myös yleisiä IoT-kameroihin liittyviä haavoittuvuuksia, joita haittaohjelmat voivat hyödyntää. Eri valmistajien IoT-kameroiden haavoittuvuuksista annetaan myös konkreettisia esimerkkejä ja esitellään niiden vaikutuksia käyttäjien tietoturvaan. Lopuksi luvussa 3 esiteltiin tunnettuja IoT-laitteiden haittaohjelmia, kuten Mirai, QBOT ja Zollard. Mirain toimintaa esitellään myös tarkemmin.

Luvussa 4 tarkasteltiin suojatoimenpiteitä IoT-kameroihin kohdistuviin tietoturvahyökkäyksiin. Aluksi käsitellään keskeisiä EU:n säädöksiä, jotka ohjaavat IoT-laitteiden tietoturvaa. Luku esitteli valmistajille ja kuluttajille käytännön suojatoi-

mia, joita voidaan toteuttaa laitteiden suojaamiseksi. Lisäksi luvussa tuodaan esiin myös edistyneempiä suojaustekniikoita, kuten koneoppimiseen perustuvia malleja.

Tutkielman ensimmäinen tutkimuskysymys pyrki selvittämään kuluttajakäyttöön suunnattujen IoT-kameroiden tietoturvahaasteita. Kuluttajakäyttöön suunnatut IoT-kamerat altistuvat useille tietoturvahaasteille, jotka liittyvät erityisesti puutteellisiin oletusasetuksiin, heikkoihin salasanoihin, salaamattomaan tiedonsiirtoon ja valmistajien riittämättömään ohjelmistopäivitystukeen. Monissa tapauksissa kamerat käyttävät edelleen vanhentuneita tiedonsiirtoprotokollia, kuten Telnetiä ja HTTP:tä, jotka mahdollistavat välitetyn tiedon sieppaamisen. Lisäksi laitteet voivat olla alttiita haittaohjelmille, jotka hyödyntävät tunnettuja haavoittuvuuksia ja oletussalasanoja. Mirai on yksi esimerkki tällaisesta haittaohjelmasta. Kuluttajien tietoturvaan vaikuttavat myös hallintasovellusten ja pilvipalveluiden haavoittuvuudet, joiden kautta hyökkääjät voivat saada pääsyn kamerakuvaan tai henkilötietoihin. Nämä tietoturvahaasteet saattavat korostua erityisesti tilanteissa, joissa käyttäjällä ei ole teknistä osaamista tai tietoisuutta tietoturvasta.

Tutkielman toinen tutkimuskysymys pyrki selvittämään suojatoimenpiteitä IoT-kameroiden tietoturvan parantamiseksi. IoT-kameroiden tietoturvaa voidaan parantaa useilla teknisillä toimenpiteillä. Kuluttajan näkökulmasta keskeisiä toimia ovat oletussalasanojen vaihtaminen vahvoihin salasanoihin, ohjelmistopäivitysten säännöllinen asentaminen sekä laitteiden sijoittaminen fyysisesti turvallisiin paikkoihin. Myös vanhentuneiden tiedonsiirtoprotokollien käytön rajoittaminen tai poistaminen voi merkittävästi parantaa suojaustasoa. Kehittäjien ja valmistajien vastuulla on puolestaan hyödyntää vahvoja salausmenetelmiä, suorittaa säännöllistä tietoturvatestausta sekä tarjota käyttäjäystävällisiä päivitysratkaisuja. Lisäksi koneoppimisen ja syväoppimisen menetelmiä voidaan hyödyntää haitallisen liikenteen havaitsemisessa eri IoT-arkkitehtuurin tasoilla. Lainsäädännön ja sertifiointien avulla voidaan pyrkiä ohjaamaan alan toimijoita kohti turvallisempia IoT-järjestelmiä ja esimerkik-

si GDPR:n ja EU:n kyberturvallisuusasetuksen tarkoituksena on ohjata valmistajia kehittämään laitteiden tietoturvaa.

Lähdeluettelo

[1] B. Tripathy ja J. Anuradha, *Internet of things (IoT): technologies, applications, challenges and solutions*. CRC press, 2018. DOI: 10.1201/9781315269849.

[2] Z. Trabelsi, "Investigating the Robustness of IoT Security Cameras against Cyber Attacks", teoksessa *2022 5th Conference on Cloud and Internet of Things (CIoT)*, 2022, s. 17–23. DOI: 10.1109/CIoT53061.2022.9766814.

[3] J. Li, "Cyber-attacks on cameras in the IoT networks", teoksessa *2021 2nd International Conference on Computer Communication and Network Security (CCNS)*, 2021, s. 94–97. DOI: 10.1109/CCNS53852.2021.00027.

[4] F. Meneghello, M. Calore, D. Zucchetto, M. Polese ja A. Zanella, "IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices", 5, vol. 6, 2019, s. 8182–8201. DOI: 10.1109/JIOT.2019.2935189.

[5] P. Fremantle ja P. Scott, "A survey of secure middleware for the Internet of Things", vol. 3, PeerJ Inc., 2017, e114. DOI: 10.7717/peerj-cs.114.

[6] S. M. Brundha, P. Lakshmi ja S. Santhanalakshmi, "Home automation in client-server approach with user notification along with efficient security alerting system", teoksessa *2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon)*, 2017, s. 596–601. DOI: 10.1109/SmartTechCon.2017.8358441.

[7] M. A. El. zuway ja H. M. Farkash, ”Internet of Things Security: Requirements, Attacks on SH-IoT Platform”, teoksessa *2022 IEEE 21st international Ccnference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)*, 2022, s. 742–747. DOI: 10.1109/STA56120.2022.10019124.

[8] S. Khanam, I. B. Ahmedy, M. Y. Idna Idris, M. H. Jaward ja A. Q. Bin Md Sabri, ”A Survey of Security Challenges, Attacks Taxonomy and Advanced Countermeasures in the Internet of Things”, vol. 8, 2020, s. 219 709–219 743. DOI: 10.1109/ACCESS.2020.3037359.

[9] T. Alladi, V. Chamola, B. Sikdar ja K.-K. R. Choo, ”Consumer IoT: Security Vulnerability Case Studies and Solutions”, 2, vol. 9, 2020, s. 17–25. DOI: 10.1109/MCE.2019.2953740.

[10] V. Visoottiviseth, T. Khengthong, K. Kesorn ja J. Patcharadechathorn, ”ASPAHI: Application for Security and Privacy Awareness Education for Home IoT Devices”, teoksessa *2021 25th International Computer Science and Engineering Conference (ICSEC)*, 2021, s. 388–393. DOI: 10.1109/ICSEC53205.2021.9684659.

[11] V. Visoottiviseth, C. Kotarasu, N. Cheunprapanusorn ja T. Chamornmarn, ”A Mobile Application for Security Assessment Towards the Internet of Thing Devices”, teoksessa *2019 IEEE 6th Asian Conference on Defence Technology (ACDT)*, 2019, s. 1–7. DOI: 10.1109/ACDT47198.2019.9072921.

[12] O. Almazrouei, P. Magalingam, M. Kamrul Hasan, M. Almehrzi ja A. Alshamsi, ”Penetration Testing for IoT Security: The Case Study of a Wireless IP Security CAM”, teoksessa *2023 IEEE 2nd International Conference on AI in Cybersecurity (ICAIC)*, 2023, s. 1–5. DOI: 10.1109/ICAIC57335.2023.10044176.

[13] C. Kelly, N. Pitropakis, S. McKeown ja C. Lambrinoudakis, "Testing And Hardening IoT Devices Against the Mirai Botnet", teoksessa *2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 2020, s. 1–8. DOI: 10.1109/CyberSecurity49315.2020.9138887.

[14] CCTV Calculator. "Vulnerability database". (2025), url: https://www.cctvcalculator.net/en/knowledges/vulnerability-database/ (viitattu 12. 05. 2025).

[15] P. Biondi, S. Bognanni ja G. Bella, "Vulnerability Assessment and Penetration Testing on IP camera", teoksessa *2021 8th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, 2021, s. 1–8. DOI: 10.1109/IOTSMS53705.2021.9704890.

[16] G. Gallopeni, B. Rodrigues, M. Franco ja B. Stiller, "A Practical Analysis on Mirai Botnet Traffic", teoksessa *2020 IFIP Networking Conference (Networking)*, 2020, s. 667–668.

[17] Official Journal of the European Union, "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)", 2016.

[18] Official Journal of the European Union, "REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)", 2019.

[19] Official Journal of the European Union, "DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December

2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)", 2022.

[20] H.-S. Ham, H.-H. Kim, M.-S. Kim ja M.-J. Choi, "Linear SVM-based android malware detection for reliable IoT services", 1, vol. 2014, Wiley Online Library, 2014, s. 594 501.

[21] G. Thamilarasu ja S. Chawla, "Towards deep-learning-driven intrusion detection for the internet of things", 9, vol. 19, MDPI, 2019, s. 1977.

[22] Y. Shi, Y. E. Sagduyu, T. Erpek, K. Davaslioglu, Z. Lu ja J. H. Li, "Adversarial Deep Learning for Cognitive Radio Security: Jamming Attack and Defense Strategies", teoksessa *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2018, s. 1–6. DOI: 10.1109/ICCW.2018.8403655.