Suoritettava tietoturvasertifikaatti

Juha Röning ja Rauli Kaksonen

Publications of the Scientific Advisory Board for Defence
2024:3

Maanpuolustuksen tieteellisen neuvottelukunnan julkaisuja 2024:3

Suoritettava tietoturvasertifikaatti

Juha Röning ja Rauli Kaksonen

Puolustusministeriö Helsinki 2024

Julkaisujen jakelu
Distribution av publikationer

Valtioneuvoston julkaisuarkisto Valto

Publikations-arkivet Valto

julkaisut.valtioneuvosto.fi

ISBN pdf: 978-951-663-138-0
ISSN pdf: 2984-102X

Taitto: Valtioneuvoston hallintoyksikkö, Julkaisutuotanto

Helsinki 2024

Kuvailulehti
5.2.2024

Suoritettava tietoturvasertifikaatti

Maanpuolustuksen tieteellisen neuvottelukunnan julkaisuja 2024:3

Julkaisija	Puolustusministeriö		
Tekijät	Juha Röning, Rauli Kaksonen		
Yhteisötekijä	Oulun yliopisto		
Kieli	Suomi	**Sivumäärä**	21

Tiivistelmä

Laitteiden ja palvelujen kyberturvallisuus on osa yhteiskunnan häiriötöntä toimintaa. Usein turvallisuus todennetaan tietoturvasertifikaatilla, esimerkkinä Common Criteria. Sertifikaatti kattaa kuitenkin usein vain tuotteen yhden version. Tämä ei vastaa nykyajan vaatimuksia, koska tuotteita on päivitettävä säännöllisesti. Uhat ja tekniikat päivittyvät, mihin pitäisi reagoida ripeästi. Sertifikaatin tulisi kattaa tuotteen koko elinkaari.

Tässä hankkeessa tutkittiin uudentyyppisen suoritettavan tietoturvasertifikaatin vaatimuksia ja kattavuutta. Suoritettava sertifikaatti koostuu tuotteelle räätälöidyistä ajettavista testeistä. Uudet versiot sertifioidaan ajamalla testitapaukset uudelleen. Hankkeessa toteutettiin kaksi prototyyppiä todelliselle tuotteelle. Ensimmäisen prototyypin vaatimuskattavuus on 80 % tutkimuksesssa laadituille vaatimuksille. Toinen prototyyppi käytti ETSI EN 301 645 -standardia, ja saavutti 45 %:n kattavuuden tietoturvakriittisilille rajapintatesteille. Korkeampi automaatioaste on mahdollista saavuttaa lisätyöllä.

Suoritettava tietoturvasertifikaatti voidaan toteuttaa, mutta ainakaan aluksi se ei kata kaikkia vaatimuksia. Kattavuutta voidaan laajentaa kehittämällä vaatimuksia ja käytettyjä tekniikoita. Suoritettava sertifikaatti mahdollistaisi tuotteiden elinkaaren kattavan sertifioinnin, mikä nostaisi yleistä tietoturvan tasoa.

Klausuuli Tämä julkaisu on toteutettu osana Maanpuolustuksen tieteellisen neuvottelukunnan (MATINEn) tutkimusrahoituksen toimeenpanoa. (www.defmin.fi/matine) Julkaisun sisällöstä vastaavat tiedon tuottajat, eikä tekstisisältö välttämättä edusta puolustusministeriön näkemystä.

Asiasanat maanpuolustus, tutkimus, kokonaismaanpuolustus, esineiden internet, tietoturva, kyberturvallisuus, sertifikaatit, tietoturvavaatimus, testaus

ISBN PDF	978-951-663-138-0	**ISSN PDF**	2984-102X
Julkaisun osoite	https://urn.fi/URN:ISBN:978-951-663-138-0		

Presentationsblad
5.2.2024

Exekverbart cybersäkerhetscertifikat

Publikationer av försvarets vetenskapliga delegation 2024:3

Utgivare	Försvarsministeriet		
Författare	Juha Röning, Rauli Kaksonen		
Utarbetad av	Uleåborg universitet		
Språk	Finska	**Sidantal**	21

Referat

Cybersäkerhet för enheter och tjänster är en del av det oavbrutna samhällets funktion. Ofta verifieras säkerheten med ett cybersäkerhetscertifikat, såsom Common Criteria. Dock täcker ett certifikat vanligtvis endast en produktversion. Detta uppfyller inte dagens standarder, som kräver regelbundna uppdateringar. Hot och tekniker utvecklas, vilket bör hanteras i tid. Ett certifikat bör täcka hela produktens livscykel.

Detta projekt undersökte krav och täckning för ett nytt exekverbart cybersäkerhetscertifikat. Ett exekverbart certifikat består av tester som bedömer säkerheten. En ny version certifieras genom att köra om testerna. Två prototypcertifikat implementerades för en produkt i verkliga världen. Det första prototypcertifikatet uppnådde 80 % täckning för krav utvecklade i studien. Det andra prototypen använde standarden ETSI EN 301 645 och uppnådde 45 % täckning för kritiska gränssnittsäkerhetstester. En högre täckning är uppnåelig med ytterligare arbete.

Ett exekverbart säkerhetscertifikat kan implementeras. Dock är det åtminstone till en början osannolikt att det täcker alla krav. Täckningen kan utökas genom att förbättra kraven och de använda teknikerna. Ett exekverbart certifikat skulle möjliggöra certifiering som täcker hela produktlivscykler, vilket leder till en bättre övergripande cybersäkerhetssituation.

Klausul

Den här publikation är en del i genomförandet av forskningsfinansiering av Försvarets vetenskapliga delegation. (www.defmin.fi/matine) De som producerar informationen ansvarar för innehållet i publikationen. Textinnehållet återspeglar inte nödvändigtvis statsrådets ståndpunkt.

Nyckelord

försvaret, forskning, totalförsvaret, Sakernas Internet, Säkerhet, Cybersäkerhet, Certifikat, Säkerhetskrav, Testning

ISBN PDF	978-951-663-138-0	**ISSN PDF**	2984-102X
URN-adress	https://urn.fi/URN:ISBN:978-951-663-138-0		

Description sheet
5 February 2024

Executable cybersecurity certificate

Publications of the Scientific Advisory Board for Defence 2024:3

Publisher	Ministry of Defence		
Authors	Juha Röning, Rauli Kaksonen		
Group author	University of Oulu		
Language	Finnish	**Pages**	21

Abstract

Cybersecurity of devices and services is part of the uninterrupted functioning of society. Often, security is verified with a cybersecurity certificate, such as the Common Criteria. However, a certificate typically covers only one product version. This does not meet today's standards, which call for regular updates. Threats and techniques evolve, which should be timely addressed. A certificate should cover the entire product lifecycle.

This project investigated the requirements and coverage of a novel executable cybersecurity certificate. An executable certificate comprises tests that assess security. A new version is certified by re-running the tests. Two prototype certificates were implemented for a real-world product. The first prototype certificate achieved 80% coverage for requirements developed in the study. The second prototype used the ETSI EN 301 645 standard and achieved 45% coverage for critical interface security tests. A higher coverage is achievable with additional work.

An executable security certificate can be implemented. However, at least initially, it is unlikely to cover all requirements. Coverage can be expanded by improving the requirements and used techniques. An executable certificate would enable certification to cover the entire lifecycles of products, leading to a better overall cybersecurity situation.

Provision This publication is part of the implementation of research funding of the Scientific Advisory Board for Defence (MATINE). (www.defmin.fi/matine) The content is the responsibility of the producers of the information and does not necessarily represent the view of the Defence Ministry.

Keywords national defence, research, comprehensive defence approach, Internet of Things, security, cybersecurity, certificates, security requirement, testing

ISBN PDF	978-951-663-138-0	**ISSN PDF**	2984-102X
URN address	https://urn.fi/URN:ISBN:978-951-663-138-0		

Sisältö

1 Johdanto

Huolehtimalla laitteiden ja palvelujen kyberturvallisuudesta turvataan osaltaan yhteiskunnan häiriötöntä toimintaa. Tuotteen turvallisuutta voidaan mitata riippumattoman tahon myöntämällä tietoturvasertifikaatilla, kuten Common Criteria (ISO/IEC 15408), ISASecure/IEC 62443 tai UL2900 [CC, ISASecure, UL2900]. Kyberturvallisuuskeskus tarjoaa lakisääteistä arviointi- ja hyväksymispalvelua kriittisille tuotteille [Traficom2017]. Tietoturvamerkki on kevyempi kuluttajatuotteisiin suunnattu hyväksyntä, joka perustuu ETSI EN 303 645 -standardiin [Tietoturvamerkki, ETSI-EN-303-645].

Sertifikaatti koskee yleensä vain tuotteen yhtä versiota. Tuotetta pitäisi kuitenkin voida päivittää, erityisesti, jos siitä löytyy haavoittuvuuksia. Ongelma voidaan välttää sertifioimalla tuotteen sijasta organisaatio, työmenetelmät tai työntekijät, mutta tällöin itse tuotetta ei tutkita. Toinen vaihtoehto on sallia päivitetyn version hyväksyntä kevennetyllä prosessilla.

Testaus on keskeinen tuotteen laatutekijä. Tämä pätee myös tietoturvaan. Esimerkiksi Common Criteria sisältää valmistajan testitapausten tarkastelua. Sertifikaatit voivat edellyttää tiettyjä työkaluja. Esimerkiksi ISASecure edellyttää Nessus-työkalun ja hyväksytyn fuzzing-työkalun käyttöä. SIP-protokollalle on määritelty SIP Torture Tests [RFC4475]. ETSI TS 103 301 sisältää valmiit testitapaukset mainittuun ETSI EN 303-645 -standardiin [ETSI-TS-103-701]. Viime aikoina ohjelmistojen kehityksessä on otettu tavoitteeksi jatkuva integraatio ja jopa jatkuva julkaiseminen (CI/CD), mikä vaatii testauksen automatisointia.

Toimittajan, asiakkaan ja sertifioijan välisen suhteen ongelmana on, että tuotetta ei tarkastella osana asiakkaan järjestelmää eikä koko tuotteen elinkaaren ajan [Huopio2021]. Sertifiointi, joka kohdistuu vain tuotteen tiettyyn versioon, ei vastaa nykyajan vaatimuksia. Tietoturvatestauksen pitäisi olla jatkuvaa ja automaattista. Sertifikaattia itsessään pitäisi myös päivittää vastaamaan uusimpiin hyökkäys- ja puolustustekniikoihin.

2 Tutkimuksen tavoite ja tutkimussuunnitelma

2.1 Taustaa

Tietoturvan tason selvittämiseksi on tunnettava hyökkäys- ja puolustustekniikat [Cho2019, Stellios2018]. Usein tietomurron mahdollistavat vanhat tai turvattomat laitteet, päivitysten puute ja puuttuva salaus tai pääsyn hallinta [Stergiopoulos2020]. Laitteiden valmistajat keskittyvät usein uusiin ominaisuuksiin tietoturvan kustannuksella [Chaabouni2019]. Tietoturvavaatimukset vaihtelevat alan ja näkökulman mukaan. Tange, et al. listaa tärkeimmiksi tietoturvan monitoroinnin, datan turvallisen säilytyksen, molemminpuolisen autentikoinnin ja tietoturvallisen suunnittelun [Tange2020]. Stellios, et al. listaa 16 eri kontrollia [Stellios2018].

Sertifioinnin ongelma on usein prosessin hitaus [Ferreira2017]. Sertifiointi kohdistuu joko tuotteeseen, kehitysprosessiin, organisaatioon, tai ihmisiin [Ramires2020, Voas2018]. Jatkuvaa ja automaattista sertifiointia on ehdotettu pilvipalveluille [Kunz2017]. Prosessien, työkalujen tai ihmisten sertifiointi ei ole tae lopputuloksena syntyvän laitteen laadusta [Voas2000]. Tarkastelu tulisikin kohdistua tuotteen ominaisuuksiin käyttäen tehokkaita ja toistettavia menetelmiä. Testausta pohdittaessa on hyvä huomata, että avoimen lähdekoodin työkaluja on saatavilla monille tietoturvan osa-alueille [Kaksonen2021].

2.1.1 Tavoite ja sisältö

Hankkeen tavoitteena oli määrittää vaatimukset uudenlaiselle suoritettavalle tietoturvasertifikaatille, jolla voidaan varmentaa tuotteen tietoturvaa sen koko elinkaaren ajan. Sertifikaatti koostuu ajettavista tietoturvatesteistä. Suoritettava sertifikaatti luo uuden paradigman, jossa tuotteen yhden version sijasta sertifioidaan tuotteelle räätälöidyt ajettavat tietoturvatestit. Sertifiointi kattaa tuotteen koko elinkaaren ja testejä voidaan tarvittaessa lisätä. Hanke yhdistää testauksen, tietoturvatyökalut ja tietoturvan sertifioinnin tavalla, joka lisää tietoturvan läpinäkyvyyttä.

Suoritettavan sertifikaatin luo joko tuotteen valmistaja, sertifioija tai joku muu taho, mutta sertifikaatin hyväksyy riippumaton taho. Sertifikaatin ajaminen on tämän jälkeen mahdollista kohtuullisella vaivalla kenelle tahansa, jolla on pääsy vaadittavaan materiaaliin.

Tietoturva-asiantuntijat suunnittelevat testitapaukset, joista sertifikaatti koostuu. Testeissä käytetään yleisiä, mieluiten avoimen lähdekoodin, tietoturvatyökaluja, jotka pakataan esimerkiksi Docker-kontteihin (containers). Ajettavuus on suuri etu verrattuna perinteiseen sertifikaattiin. Tuotteen uusi versio voidaan sertifioida ajamalla testitapaukset uudelleen. Tämä ei kata tuotteen uusia ominaisuuksia, mutta niitä varten voidaan lisätä uusia testitapauksia. Suoritettava sertifikaatti voidaan ajaa tuotteen eri konfiguraatioille ja eri ympäristöissä. Sertifikaattiin voidaan lisätä löydettyjen haavoittuvuuksien tarkistuksia, jolloin sertifikaatti tukee tietoturvan päivittämistä.

Tutkimuksessa kartoitimme tietoturvaominaisuuksia ja työkaluja, joita on saatavilla tietoturvan testaamiseen. Testatut vaatimukset koottiin analysoimalla standardeja, -ohjeita, parhaita käytäntöjä ja alan tutkimusta [CC, ISASecure, ETSI-EN-303-645]. Projetissa hyödynsimme aiempia tutkimuksiamme avoimen lähdekoodin tietoturvatyökaluista ja IoT-tietoturvavaatimuksista [Kaksonen2021, Kaksonen2022]. Toteuttavuutta tutkimme rakentamalla kaksi erilaista sertifikaattia todelliselle tuotteelle. Keskeisimpänä mittarina tarkastelimme, kuinka moni vaatimus voidaan testata suoritettavalla sertifikaatilla.

2.1.2 Tutkimuksen suoritus ja vaiheet

Tutkimus suoritettiin Oulun yliopistossa Tietoturvallisen ohjelmoinnin tutkimusryhmässä (OUSPG) vuosina 2022–2023. Hankkeen vastuullinen johtaja on Oulun yliopiston professori Juha Röning. Hankkeen tutkimusta vetää Rauli Kaksonen, erityisasiantuntija, tietoturva. Projektissa on kolme eri tutkimustehtävää. Tehtävien kuvaukset projektisuunnitelmasta on esitetty Taulukossa 1.

Taulukko 1. Tutkimustehtävien kuvaus projektisuunnitelmasta.

Tehtävä	Kuvaus
Tietoturva-vaatimusten kartoitus	Tehtävässä kartoitetaan suoritettavalta tietoturvasertifikaatilta vaadittavia ominaisuuksia. Kartoituksessa analysoidaan tietoturvastandardeja, -ohjeita ja parhaita käytäntöjä sekä alan tutkimuksia. Tulos: Tutkimus tärkeimmistä tietoturvavaatimuksista (raportti/artikkeli).
Työkalu- ja teknologia-valinnat	Tehtävässä kartoitetaan suoritettavalta tietoturvasertifikaatilta vaadittavia ominaisuuksia. Kartoituksessa analysoidaan tietoturvastandardeja, -ohjeita ja parhaita käytäntöjä sekä alan tutkimuksia. Tulos: Tutkimus tärkeimmistä tietoturvavaatimuksista (raportti/artikkeli)
Prototyyppi ja tulosten validointi	Tehtävässä valittu lähestyminen validoidaan toteuttamalla sertifikaatin prototyypit 1–2 tuotteelle, jotka valitaan hankkeen aikana. Prototyyppejä toteutetaan kaksi, joista ensimmäinen luotaa käytettäviä tekniikoita ja toinen koko konseptin toteutettavuutta. Työmäärää, kattavuutta ja käytettävyyttä mitataan suhteessa tehtävän 1 tuloksiin ja arvioidaan yhdessä sidosryhmien kanssa. Tulos: Kaksi prototyyppiä suoritettavasta sertifikaatista ja arviointiraportti

3 Tulokset

Seuraavissa kappaleissa esitellään Suoritettava tietoturvasertifikaatti -projektin keskeisimmät tulokset. Tutkimusongelmaa lähestytään esineiden internetin, IoT (Internet of Things), konseptin kautta [IoT]. IoT:lla viitataan yleensä tapaan, jolla erilaiset laitteet yhdistetään internetin, tai muiden verkkojen, kautta toisiinsa ja taustajärjestelmiin. Tavoitteena on luoda ”älykkäitä” järjestelmiä, joiden avulla luodaan uusia palveluja, tehostetaan resurssien käyttöä, automatisoida rutiinitehtäviä, jne. Esimerkkinä vaikka auto, jonka toimintoja voi hallita matkapuhelimella, tai valvontakamera, joka mahdollistaa etävalvonnan internetin yli.

IoT ei ole tulevaisuuden visio, vaan se on jo täällä. Arkemme ja Suomen kriittinen infrastruktuuri on jo suurelta osin rakennettu erilaisten IoT-järjestelmien avulla. Tästä syytä IoT-tietoturva on erittäin tärkeää ja mielekäs tapa jäsentää tätä tutkimusta. Tulokset ovat sinänsä yleistettävissä muihinkin informaatioteknologian (IT) tuotteisiin, joissa ei ole osana laitteistoja.

3.1 Tietoturvavaatimukset

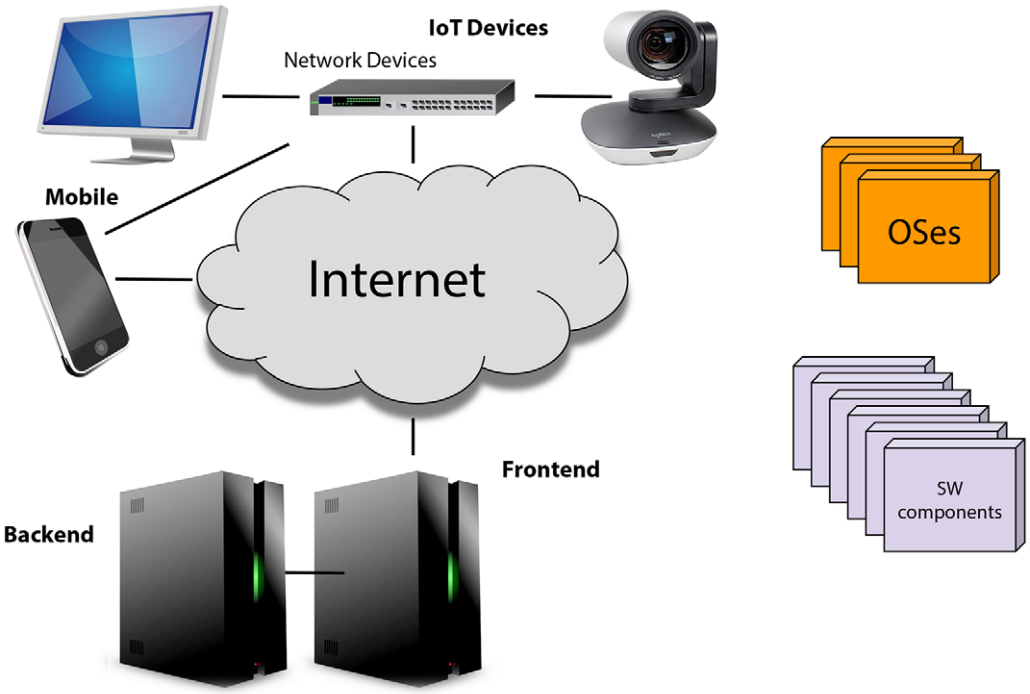
Projektissa hyödynnettiin aiempaa tutkimustamme yleisistä IoT-tietoturvavaatimuksista [Kaksonen2022]. Tutkimuksessa käytiin läpi 16 eri IoT-tietoturvavaatimuskokoelmaa ja tunnistettiin yleisimmät vaatimuskategoriat. Seuraavat kategoriat löydettiin kaikista tutkituista vaatimuslähteistä:

- Tietoturva-arkkitehtuurin määrittely,
- järjestelmän rajapintojen suojaus,
- datan suojaus,
- käyttäjien ja komponenttien tunnistaminen ja
- ohjelmistojen päivitys.

Projektissa kartoitettiin myös IoT-haavoittuvuuksia ja niiden esiintyvyys alijärjestelmissä. Tutkimustapa oli National Vulnerability Database:ssa (NVD) esiintyvän haavoittuvuustiedon luokittelu ja analysointi. NVD sisältää tietoa ympäri maailmaa raportoiduista haavoittuvuuksista, ja se on suurin ja tunnetuin haavoittusvuustietokanta. Tutkimuksessa analysoitiin n. 500 haavoittuvuusraporttia, joista tunnistettiin

haavoittuva alijärjestelmä, hyökkäysvektori sekä haavoittuvuuden tyyppi. NVD:n raportoidaan yli 20 000 haavoittuvuutta vuodessa, joten analyysiin poimittiin vain pieni osa kokonaisuudesta.

Kuvio 1. Esineiden internetin, Internet of Things (IoT), alijärjestelmät.



Kuviossa 1 esitellään IoT:n alijärjestelmät, joiden avulla haavoittuvuuksia luokiteltiin. Tutkimuksessa IoT-järjestelmät jaettiin seuraaviin alijärjestelmiin: IoT-laitteet (Devices), taustajärjestelmän verkkorajapinta (Frontend) ja sisäiset osat (Backend), mobiilisovellukset (Mobile), käyttöjärjestelmät (OS), ja yleiskäyttöiset ohjelmistokomponentit (SW components). IoT-laitteet jaettiin lisäksi varsinaisiin IoT-laitteisiin ja verkkolaitteisiin (Network devices).

NVD sisältää haavoittuvuuksia kaikista alijärjestelmissä käytetyistä komponenteista. Määrällisesti taustajärjestelmiin liittyvistä komponenteista raportoidaan enemmän haavoittuvuuksita kuin IoT-laitteisiin tai mobiilisovelluksiin liittyvistä. Seuraavassa vedetään yhteen IoT-haavoittuvuustutkimuksen keskeisimmät löydökset.

- Lähes 90 % kaikista raportoiduista haavoittuvuuksista koskettaa IoT-järjestelmiä, yleensä ohjelmistokomponentteja, joista eri alijärjestelmät koostuvat
- Raportoiduista haavoittuvuuksista yli 50 % on taustajärjestelmissä, 13 % käyttöjärjestelmissä, 10 % IoT-laitteissa, 1 % mobiilisovelluksista ja 15 % yleiskäyttöisissä ohjelmistokomponenteissa. Poimimalla haavoittuvuuksia eri tavoin päädytään hieman erilaisiin osuuksiin.
- Kaikkia IoT-alijärjestelmiä pitäisi voida päivittää näiden haavoittuvuuksien korjaamiseksi. Tämä vaatii komponenttien listaamista (ns. Software Bill of Materials, SBOM)
- Yleisin haavoittuva komponentti on HyperText Transport Protocol (HTTP) palvelimet, joita on sekä IoT-laitteissa että taustajärjestelmissä. Haavoittuvuuksia löytyy myös muista verkko-ohjelmistoista.

Yksityiskohtaiset tulokset on esitelty julkaisussa [Kaksonen2023-1].

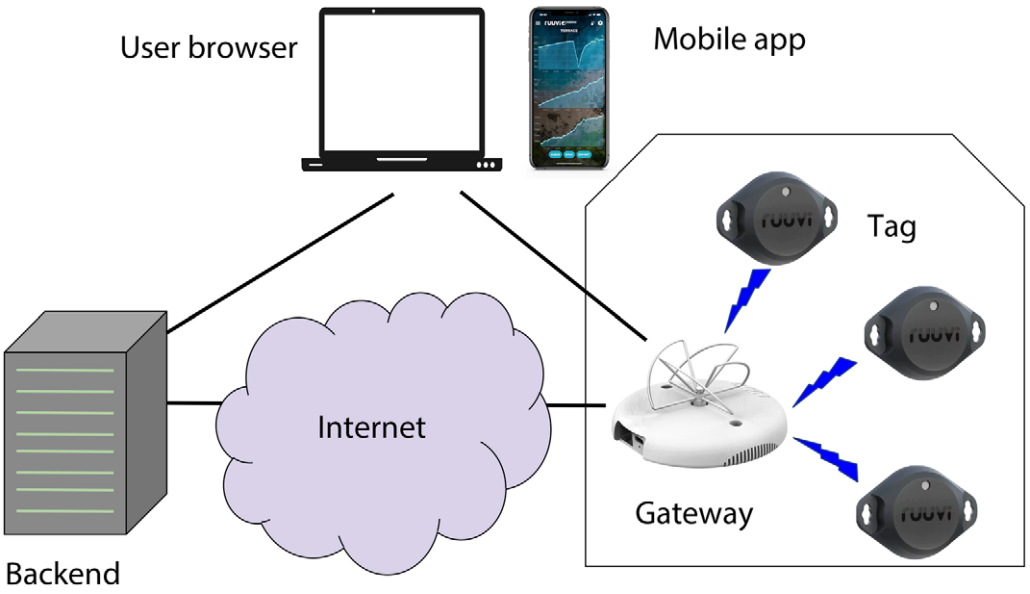
3.2 Työkalu- ja teknologiavalinnat

Suoritettava sertifikaatti perustuu tietoturvatyökaluihin, joka suorittavat varsinaisen testauksen. Suuri osa näistä työkaluista voi olla avoimen lähdekoodin vapaasti käytettäviä työkaluja. Avoimen lähdekoodin työkalut edustavat usein parasta saatavilla olevaa teknologiaa. Näitä työkaluja on laajasti saatavilla erilaisiin tarpeisiin [Kaksonen2021]. Niiden vapaa käytettävyys on etu koska sertifikaatin ajaminen ei vaadi lisensointia.

3.2.1 Prototyyppi ja tulosten validointi

Projektin aikana rakennettiin Python-ohjelmointikielellä demonstraatiojärjestelmä. Prototyypillä toteutettiin suoritettavan sertifikaatin prototyyppi Ruuvi Oy:n IoT-tuotteille Ruuvi Gateway ja Ruuvi Tags [Ruuvi]. Tuotteella on suomalainen Tietoturvamerkki [RuuviTTM]. Kuvio 2 havainnollistaa tuotteiden arkkitehtuuria. Ruuvi Tag:it lähettävät mittaustietoa Gateway:lle joka välittää sen internetin kautta taustajärjestelmälle (Backend). Käyttäjä konfiguroi Gateway:tä selaimella. Taustajärjestelmään siirrettyä mittaustietoa voi myös tarkastella selaimella tai mobiilisovelluksella.

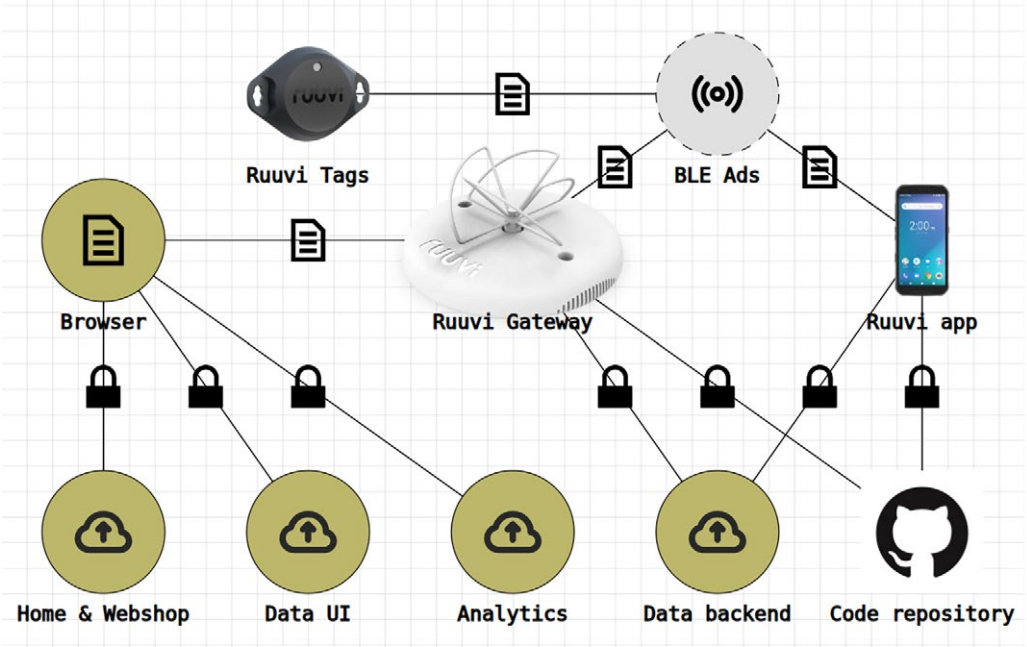
Kuvio 2. Ruuvi Gateway ja Tags-tuotteen arkkitehtuuri.



Suoritettavasta sertifikaatista tehtiin kaksi eri versiota. Ensimmäinen käyttäen tietoturvavaatimuksia, jotka ovat johdettu edellä mainituista tutkimuksista. Toisessa vaatimuksen poimittiin kuluttajasektorin IoT-tietoturvastandardista ETSI EN 303 645 [ETSI-EN-303-645] ja erityisesti sen testispesifikaatiosta ETSI TS 103 701 [ETSI-TS 103-701].

Ensimmäiseksi Ruuvituotteesta luotiin kuvaus, josta käytämme englanninkielistä termiä security statement. Kuvaus sisältää tietoturvan kannalta oleelliset piirteet, mm. tietoturva-arkkitehtuurin. Kuvauksen pitää sisällyttää tieto, jonka avulla voidaan verifioida standardin vaatimusten toteutus. Kuvio 3 näyttää kuvauksesta johdetun järjestelmän visualisoinnin, josta näkee verkkosolmut ja niiden väliset tärkeimmät yhteydet.

Kuvio 3. Ruuvi Gateway ja Tags-kuvauksesta johdettu visualisointi



Kun järjestelmäkuvaus on valmis, voidaan rakentaa automaatio, joka tarkistaa, että kuvaus on todenmukainen. Ensimmäisen prototyypin tietoturvavaatimukset ja niiden testaukseen käytetyt työkalut on listattu taulukossa 3. Vaatimusten, työkalujen ja menetelmien kuvaukset löytyvät julkaisusta [Kaksonen2023-2]. Työkalujen avulla toteutetulla automaatiolla saavutettiin 80 % kattavuus, kun tarkastellaan eri mitattavia kohteita ja niihin kohdistettuja vaatimuksia.

Taulukko 2. Suoritettavan sertifikaatin prototyypin automaation kattavuus Ruuville.

Vaatimus	Autom.	Työkalu tai metodi
Verkkosolmut määritelty	10/10	Nmap, Censys, Tcpdump
Verkkopalvelut määritelty	12/12	Nmap, Censys, Tcpdump
Verkkoyhteydet määritelty	8/9	Tcpdump, HAR, HCIdump
Protokollien parhaat käytännöt, TLS	5/5	Testssh.sh
Protokollien parhaat käytännöt, SSH	2/2	Ssh-audit
Web parhaat käytännöt	5/6	Censys, ZED, HAR

Vaatimus	Autom.	Työkalu tai metodi
Palvelujen autentikaatio	0/4	Manuaalinen
Yhteyksien salaus	6/7	Tcpdump
Yksityinen data määritelty	0/3	Manuaalinen
Yksityisyyspolitiikka määritelty	1/1	Web-sivun tarkistus
Päivitykset salaisia ja automaattisia	1/1	Tcpdump
SBOM määritelty	1/3	Black Duck
Ei tunnettuja haavoittuvuuksia	1/3	Black Duck
Tietoturvapolitiikka määritelty	1/1	Web-sivun tarkistus
Päivityshistoria saatavilla	3/3	Gitlab API
Sovelluksen oikeudet määritelty	1/1	APKPure, Apktool
Automaatiokattavuus	**57/71**	**80 %**

Toisessa prototyypissä käytettiin vaatimuksia ETSI EN 303 645 standardista. Näille vaatimuksille on määritelty testitapaukset spesifikaatiossa ETSI TS 103 701. ETSI EN 303 645 rajoittaa tarkastelun IoT-laitteisiin ja niiden yhteyksiin, joten taustajärjestelmiä ja mobiilisovelluksia ei testata. Tutkimuksen valossa tämä rajaus jättää ison osan kokonaisjärjestelmän tietoturvasta sertifioinnin ulkopuolelle.

ETSI TS 103 701 spesifikaation 226 testiä jaettiin erilaisiin kategorioihin. Automaation kannalta oleellisiksi tunnistettiin 106 tuotetestiä, jotka testaavat itse IoT-laitetta eivätkä toimitettua dokumentaatiota. Nämä 106 tuotetestiä jakaantuivat vielä 56 tietoturvan rajapintatestiksi ja 50 käyttöliittymätestiksi. Tutkimuksessa keskityttiin 56 rajapintatestin automatisointiin. Tarkastelemalla näitä testejä todettiin, että yleisillä verkkotyökaluilla päästään 52 %:n automaatioasteeseen. Edistyneempien työkalujen avulla tämä voidaan nostaa 70 %:iin. 100 %:n kattavuus vaatii räätälöityjen työkalujen kehittämistä. Lopuksi toteutettiin prototyyppisertifikaatti em. Ruuvi-tuotteille. Tämän sertifikaatin kattavuus on 45 % tietoturvan rajapintatesteistä. Yksityiskohtaiset tulokset on esitelty julkaisussa [Kaksonen2024].

Yhteenvetona tuloksista voidaan todeta, että suoritettava sertifikaatti on mahdollinen, mutta ainakaan alkuvaiheessa se ei kata kaikkia tietoturvavaatimuksia. Nämä vaatimukset on edelleen testattava käsin. Tietoturvan testaus vaatii myös IoT-järjestelmän käyttöä, jotta sen eri ominaisuudet aktivoituvat. Esimerkiksi Ruuvi-tuote piti asentaa ja sen perustoimintoja käyttää selaimella sovelluksella. Sikäli kun käyttöliittymätoimintoja ei voida automatisoida, myös tämä jää ihmisen tehtäväksi.

Täydellisesti automatisoitujen testien osa jää siis helposti pieneksi. Tuotteen käyttö ei kuitenkaan vaadi tietoturvaosaamista, joten siinä voidaan hyödyntää tuotteelle muutenkin tehtävää testausta. Voisi myös ajatella, että sertifiointia suoritettaisiin jatkuvasti tuotteen käytön ohessa, jolloin päästään kiinni jatkuvaan sertifiointiin. Tällöin ei voida kuitenkaan käyttää niitä työkaluja, jotka häiritsevät tuotteen normaalia toimintaa. Osittainenkin tietoturvan testaus lienee kuitenkin parempi kuin vaihtoehto, jossa sitä ei testata ollenkaan.

3.3 Tieteellinen merkittävyys ja julkaisut

Projekti tuotti tieteellisesti merkittäviä tuloksia. Projektin kuluessa kirjoitettiin kolme konferenssiartikkelia:

1. Kaksonen, R., Halunen, K., & Röning, J. (2023). Vulnerabilities in IoT Devices, Backends, Applications, and Components. In ICISSP – 9th International Conference on Information Systems Security and Privacy. (p. 659-668). SciTePress. doi: 10.5220/0011784400003405
2. Kaksonen, R., Halunen, K., Laakso, M., & Röning, J. (2023). Transparent Security Method for Automating IoT Security Assessments. In The 18th International Conference on Information Security Practice and Experience (ISPEC). Springer International Publishing.
3. Kaksonen, R., Halunen, K., Laakso, M., & Röning, J. (2024). Automating IoT Security Standard Testing by Common Security Tools. In ICISSP – 10th International Conference on Information Systems Security and Privacy. Helmikuu 2023.

Julkaisimme tehtävän ”Tietoturvavaatimusten kartoitus” tulokset 1. artikkelissa, joka täydentää jo aiemmin julkaistua tutkimustamme [Kaksonen2022]. Tehtävien ”Työkalu- ja teknologiavalinnat” ja ”Prototyyppi ja tulosten validointi” tulokset julkaisimme 2. ja 3. artikkelissa. Projektin tulokset toimivat myös ytimenä Rauli Kaksosen väitöskirjalle. Väitöskirjan aineena on IoT-tuotteiden automaattinen tietoturvatestaus ja -sertifiointi yleisten tietoturvatyökalujen avulla. Väitöskirjan on tarkoitus valmistua vuoden 2024 aikana.

Projektin tuloksia on esitelty Matine-seminaareissa 2022 ja 2023 sekä Kyberturvakeskuksen järjestämässä Vulnmeet-tapahtumassa tammikuussa 2023. Lisäksi tutkimusta on esitelty lukuisissa yliopiston tilaisuuksissa. Projektin aiheesta on järjestetty yli 10 erillistä sidosryhmäpalaveria, joissa on keskusteltu tuloksista ja tutkimuksen suuntaamisesta.

3.4 Tulosten hyödyntämismahdollisuudet

Puolustusvoimat ja valtionhallinto hankkivat lukuisia tuotteita kriittisiin tehtäviin. Kyberturvallisuuskeskus tarjoaa näiden tuotteiden arviointi- ja hyväksymispalvelua. Suoritettava tietoturvasertifikaatti voisi olla osa hankinta- ja hyväksyntäprosesseja silloin, kun tietoturvan asema on korostunut. Viranomainen asettaisi sertifikaatille vaatimukset, hyväksyisi lopputuloksen ja suorittaisi hyväksyntäajot. Valmistaja tai ulkopuolinen taho tekisi varsinaiset testitapaukset.

Tehokkaampi tietoturvan sertifiointi avaa mahdollisuuden kattaa huomattavasti nykyistä laajemman joukon laitteita ja palveluja, mikä nostaisi tietoturvan yleistä tasoa ja näin hyödyttäisi koko yhteiskuntaa.

LÄHTEET

[CC] Common Criteria portal, https://www.commoncriteriaportal.org.

[Chaabouni2019] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac and P. Faruki, "Network Intrusion Detection for IoT Security Based on Learning Techniques," in IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2671-2701, thirdquarter 2019, doi: 10.1109/COMST.2019.2896380.

[Cho2019] S. Cho et al., "Cyber Kill Chain based Threat Taxonomy and its Application on Cyber Common Operational Picture," 2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), 2018, pp. 1-8, doi: 10.1109/CyberSA.2018.8551383.

[CPA] Commercial Product Assurance (CPA), National Cyber Security Center, UK. https://www.ncsc.gov.uk/information/commercial-product-assurance-cpa

[ETSI-EN-103-701] Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements v1.1.1. ETSI EN 103 701, ETSI.

[ETSI-EN-303-645] CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements, ETSI 2020.

[Ferreira2017] G. Ferreira, "Software Certification in Practice: How Are Standards Being Applied?," 2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C), 2017, pp. 100-102, doi: 10.1109/ICSE-C.2017.156.

[Hupio2021] Keskustelu, Simo Huopio / PV tutkimuskeskus, tutkimusalajohtaja. 2021-06-14.

[IoT] Wikipedia, Internet of things, https://en.wikipedia.org/wiki/Internet_of_things.

[ISASecure] ISASecure/IEC 62443 CONFORMANCE CERTIFICATION. Certifying Industrial Control System Devices and Systems. https://isasecure.org.

[Kaksonen2021] Kaksonen, R., Järvenpää T., Pajukangas J., Mahalean M., Röning J. (2021) 100 Popular Open-Source Infosec Tools. To be presented in IFIP Sec 2021, https://www.ifipsec.org/2021.

[Kaksonen2022] Kaksonen, R., Halunen, K., & Röning, J. (2022). Common Cybersecurity Requirements in IoT Standards, Best Practices, and Guidelines. In Proceedings of the 7th International Conference on Internet of Things, Big Data and Security – Volume 1: IoTBDS, (p. 149-156). SciTePress. doi: 10.5220/0011041700003194

[Kaksonen2023-1] Kaksonen, R., Halunen, K., & Röning, J. (2023). Vulnerabilities in IoT Devices, Backends, Applications, and Components. In ICISSP – 9th International Conference on Information Systems Security and Privacy. (p. 659-668). SciTePress. doi: 10.5220/0011784400003405.

[Kaksonen2023-2] Kaksonen, R., Halunen, K., Laakso, M., & Röning, J. (2023). Transparent Security Method for Automating IoT Security Assessments. In The 18th International Conference on Information Security Practice and Experience (ISPEC). Springer International Publishing.

[Kaksonen2024] Kaksonen, R., Halunen, K., Laakso, M., & Röning, J. (2024). Automating IoT Security Standard Testing by Common Security Tools. In ICISSP – 10th International Conference on Information Systems Security and Privacy. Helmikuu 2024.

[Kunz2017] I. Kunz and P. Stephanow, "A Process Model to Support Continuous Certification of Cloud Services," 2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA), 2017, pp. 986-993, doi: 10.1109/AINA.2017.106.

[Ramires2020] A. Ramirez, A. Aiello and S. J. Lincke, "A Survey and Comparison of Secure Software Development Standards," 2020 13th CMI Conference on Cybersecurity and Privacy (CMI) – Digital Transformation – Potentials and Challenges(51275), 2020, pp. 1-6, doi: 10.1109/CMI51275.2020.9322704

[RFC4475] R. Sparks, Ed. Request for Comments: 4475, Session Initiation Protocol (SIP) Torture Test Messages, 2006.

[Ruuvi] Ruuvi kotisivut, https://ruuvi.com.

[RuuviTTM] Statement of compliance for the Cybersecurity Label, 2022-06-06.

[Stergiopoul2020] G. Stergiopoulos, D. A. Gritzalis and E. Limnaios, "Cyber-Attacks on the Oil & Gas Sector: A Survey on Incident Assessment and Attack Patterns," in IEEE Access, vol. 8, pp. 128440-128475, 2020, doi: 10.1109/ACCESS.2020.3007960.

[Stellios2018] Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz and J. Lopez, "A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services," in IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3453-3495, Fourthquarter 2018, doi: 10.1109/COMST.2018.2855563.

[Tange2020] K. Tange, M. De Donno, X. Fafoutis and N. Dragoni, "A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities," in IEEE Communications Surveys & Tutorials, vol. 22, no. 4, pp. 2489-2520, Fourthquarter 2020, doi: 10.1109/COMST.2020.3011208.

[Tietoturvamerkki] Tietoturvamerkki. Liikenne- ja viestintäministeriö, Traficom. https://tietoturvamerkki.fi/

[Traficom2017] Liikenne- ja viestintävirasto Traficomin suorittamat salaustuotearvioinnit ja -hyväksynnät, 2020, Dnro 1487/651/2017, Liikenne- ja viestintäministeriö.

[UL2900] ANSI/CAN/UL Standard for Software Cybersecurity for Network-Connectable Products (2017).

[Voas2000] J. M. Voas, "Limited software warranties," Proceedings Seventh IEEE International Conference and Workshop on the Engineering of Computer-Based Systems (ECBS 2000), 2000, pp. 56-61, doi: 10.1109/ECBS.2000.839861

[Voas2018] J. Voas and P. A. Laplante, "IoT's Certification Quagmire," in Computer, vol. 51, no. 4, pp. 86-89, April 2018, doi: 10.1109/MC.2018.2141036

Puolustusministeriö
Försvarsministeriet
Ministry of Defence

MATINE

Ministry of Defence

MATINE
the Scientific Advisory Board
for Defence

Eteläinen Makasiinikatu 8, Helsinki

PO Box 31, 00131 Helsinki

defmin.fi

ISSN PDF: 2984-102X

ISBN PDF: 978-951-663-138-0