Teemu Yllikäinen

Langattoman lähiverkon tietoturvatestauksen työkalun suunnittelu ja toteutus

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

18.5.2025

Tiivistelmä

Tekijä:	Teemu Yllikäinen
Otsikko:	Langattoman lähiverkon tietoturvatestauksen työkalun suunnittelu ja toteutus
Sivumäärä:	35 sivua + 0 liitettä
Aika:	18.5.2025
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tieto- ja viestintätekniikan tutkinto-ohjelma
Ammatillinen pääaine:	Tekniikan ammattikorkeakoulututkinto
Ohjaajat:	Osaamisaluejohtaja Janne Salonen

Tässä insinöörityössä suunniteltiin ja toteutettiin Android-käyttöjärjestelmälle mobiilisovellus, jonka avulla kotikäyttäjä voi arvioida langattoman lähiverkkonsa kyberturvallisuutta ilman erityistä teknistä osaamista tai root-oikeuksia. Työn lähtökohtana olivat yleisimmät kotiverkkojen tietoturvauhat, kuten heikko salaus, WPS- tai UPnP-toimintojen riskit, sekä oletusnimien ja hallintasivujen väärinkäyttömahdollisuudet. Sovelluksessa toteutettiin useita ketjutettuja testejä, jotka hyödyntävät transformation pipeline -mallia, jossa kukin testi rikastaa tulostietoa seuraavalle vaiheelle. Tämä mahdollistaa modulaarisen, laajennettavan ja tehokkaan tietoturva-analyysin. Tulokset esitetään selkeässä raporttinäkymässä, joka sisältää riskiluokituksen, ohjeita parannuksiin sekä kotiverkolle annettavan tähtiarvion. Sovellus testattiin käytännössä ja käyttäjäkyselyn perusteella se koettiin hyödylliseksi ja käyttökelpoiseksi. Työssä esitetään myös jatkokehitysehdotuksia analytiikan syventämiseksi ja tietojen esittämisen selkeyttämiseksi.

Avainsanat: tietoturva, langaton lähiverkko, mobiilisovellus, Android, CVE, WPS, WPA, kyberturva, verkkoanalyysi

---

Abstract

Author:	Teemu Yllikäinen
Title:	Design and Implementation of a Mobile Application for Wireless Network Security Testing
Number of Pages:	35 pages + 0 appendices
Date:	18.5.2025
Degree:	Bachelor of Engineering
Degree Programme:	Degree Programme in Information and Communication Technology
Professional Major:	Information and Communication Technologies (ICTs)
Supervisors:	Director of School Janne Salonen

This bachelor's thesis presents the design and implementation of a mobile application for the Android operating system that enables home users to assess the cybersecurity of their wireless local area network without requiring advanced technical skills or root access. The work is based on common vulnerabilities in home networks, such as weak encryption, risks associated with WPS and UPnP features, and misuse of default names and administrative interfaces. The application employs a transformation pipeline model, in which each test enriches the result structure for the next phase, enabling a modular, extendable, and efficient security analysis. The final results are presented in a user-friendly report view, including risk classifications, improvement recommendations, and a star rating for the home network. The application was tested in practice, and according to user feedback, it was found to be helpful and usable. The thesis also provides development suggestions for improving analytics and refining result presentation.

Keywords: cybersecurity, wireless local area network, mobile application, Android, CVE, WPS, WPA, network analysis

Sisällys

Lyhenteet

Wi-Fi: Wireless Fidelity Langattoman IEEE 802.11 standardin mukaisen lähiverkkoteknologian kaupallinen nimi.

WLAN: Wireless Local Area Network eli langaton lähiverkko. Voi viitata muihinkin kuin IEEE 802.11 standardin lähiverkkoihin

VLAN: Virtual Local Area Network on virtuaalinen lähiverkko jossa toisistaan etäällä olevat verkot yhdistetään yhteisellä osoiteavaruudella yhdeksi verkkoympäristöksi

NAT: Network Address Translation on teknologia, jossa paikallisen verkon osoiteavaruus on eri kuin sen ulkopuolisen verkon osoiteavaruus ja yhteys ulkopuolelle reititetään esim. reitittimen kautta. Tällöin paikalliset verkkoasiakkaat näkyvät ulospäin reitittimen IP-osoiteella.

IP: Internet Protocol. Esim. IP-osoite on tapa erotella laitteet numeerisilla osoitteilla verkkoavaruudessa.

SSID: Service Set Identifier, eli verkon nimi.

BSSID: Basic Service Set Identifier eli reitittimen yksilötunnus

MAC: Media Access Control on tunnus jolla kaikki verkkolaitteet erottuu toisistaan IP kerroksen alapuolella.

IoT: Internet of Things. Termi viittaa laitteisiin jotka eivät perinteisesti ole verkossa.

CVE: Common Vulnerabilities and Exposures – julkinen tietoturvahaavoittuvuuksien tunnistejärjestelmä.

AP: Access Point eli langattoman lähiverkon tukiasema

UI: User Interface eli käyttöliittymä

NVD: National Vulnerability Database – NIST:n ylläpitämä haavoittuvuustietokanta.

WPS: Wi-Fi Protected Setup – verkon yksinkertaistettu yhdistämisprotokolla, joka voi heikentää tietoturvaa.

OUI: Organizationally Unique Identifier – MAC-osoitteen alkuosa, joka kertoo valmistajan.

MITRE: The MITRE Corporation – organisaatio, joka ylläpitää mm. CVE-järjestelmää.

1 Johdanto

Internet yhteyksien lisääntymisen seurauksena myös langattomat lähiverkot ovat yleistyneet kotiympäristöissä viimeisen parin kymmenen vuoden aikana . Niinpä tänä päivänä langaton lähiverkko löytyykin lähes joka kotitaloudesta. Tässä tutkimuksessa langattomalla lähiverkolla tarkoitetaan nimenomaan Wi-Fi-verkkoa eli IEEE 802.11 standardien mukaista langatonta lähiverkkoa. Muitakin langattomia verkkoteknologioita on mutta Wi-Fi-verkkojen yleisyyden takia olen päättänyt keskittyä nimenomaan niihin.(1)(2)

Langattomien verkkojen yleisyyden syy on niiden edullisuus ja helppous. Lähes kaikissa tietokoneissa, tableteissa, puhelimissa ja monissa kodinkoneissakin kuten televisioissa, pelikonsoleissa ja jopa pesukoneissa on tuki langattomalle wi-fi yhteydelle. Kaiken lisäksi verkon käyttöönotto on varsin helppoa ja yksinkertaista. Käytännön tasolla riittää, että kytkee laitteen internet yhteydellä varustettuun lähiverkkoon ja käynnistää laitteen. Useimmat laitteet alkavat toimia suoraan ilman erityisiä asennuksia tai asetusten asettamisia. Tässä piilee myös mahdollisuus ongelmille. Mikäli laitteen oletusasetuksia ei ole tarkoitettu tietoturvalliseen käyttöön tai käyttäjä ei yksinkertaisesti osaa määritellä laitteen asetuksia tietoturvallisuus mielessä voi kodin tärkein internet yhteys muodostaa myös suurimman kyberturvauhan. Niinpä usein onkin niin, että kodin tärkeimmän internet-yhteyden kyberturvallisuus on käyttäjien tietotaidon puutteiden takia uhattuna.(3)

Tämän insinöörityön aiheeksi onkin juuri näistä syistä valikoitunut ”Langattoman lähiverkon tietoturvatestauksen työkalun suunnittelu ja toteutus”. Työn tavoitteena on ensin määritellä tyypillisimmät tietoturvaongelmat joita kotiverkoissa esiintyy. Näiden ongelmien varalle on tarkoitus määritellä ns. parhaat käytännöt eli suositukset kaikille kotikäyttäjille, joita seuraamalla kodin langattoman verkon kyberturvallisuus olisi peruslähtökohdiltaan kunnossa. Tämän kaiken tavoitteena tuottaa käyttäjille yksinkertainen mobiilisovellus jonka

avulla kotikäyttäjä voi helposti tarkistaa oman verkkoympäristönsä kyberturvallisuuden. Koska sovelluksen kohdekäyttäjäryhmä on tavalliset kotikäyttäjät sovelluksen yksinkertaiseen käyttöön ja selkeään käyttöliittymään kiinnitettiin erityistä huomiota. Lisäksi määritellyt parhaat käytännöt on tarkoitus tuoda sovellukseen mukaan siten, että sovellus ohjaa käyttäjää huomioimaan määrittellyt parhaat käytännöt ja näin pystyy jatkossakin varmistamaan tietoturvallisen verkkoympäristön myös oma-aloitteisesti.

2 Langattomien lähiverkkojen tietoturva kotikäytössä

Wi-Fi-verkkojen tietoturvahistoria ei kaikenkaikkiaan ole kovin ruusuinen. Alunalkaen Wi-Fi -teknologia ei tukenut minkäänlaista salaustakaan vaan kaikki radioliikenne kuljetettiin ilmassa täysin salaamattomassa muodossa jota sitten radioliikenteen luonteen takia kykeni kuuntelemaan kuka tahansa. (5)

Tätä puutetta on korjattu useita kertoja parantamalla ja versioimalla salausprotokollia vuosien varrella. Erilaisia salausmenetelmiä onkin vähän laskentatavasta riippuen useita mutta näistä yleisimmin listataan WEP, WPA, WPA2 ja WPA3. Salausta jouduttiin kehittämään ja versioimaan yksinkertaisesti koska WEP ja WPA murrettiin niin nopeasti. Myös WPA2 on nykyteknologialla murrettavissa mikäli salasana on kovin yksinkertainen. (4)(6)

Valitettavasti myynnissä olevien päätelaitteiden kuten tietokoneiden ja puhelinten tuki WPA3 salaukselle – joka siis on näistä ainut menetelmä, jota ei vielä ole murrettu – ei kovin usein ole saatavilla. Niinpä usein paras vaihtoehto kotikäyttäjälle on WPA2 + WPA3 moodi mikäli sellainen kodin reitittimestä löytyy. Myös monet muut Wi-Fi -verkkojen ominaisuudet jotka on alunperin tarkoitettu helpottamaan käyttäjää ovat sittemmin osoittautuneet huonoiksi ratkaisuiksi nimenomaan kyberturvan kannalta.(7)(8)

2.1 WLAN-verkkojen arkkitehtuuri

Tyypillisen kotiverkon WLAN-arkkitehtuuri on usein varsin yksinkertainen. Yleensä kodin verkko infrastruktuuri koostuu mm. seuraavanlaisista laitteista:

- Access Point (AP) eli suomeksi tukiasema. Tukiaseman tehtävän on reitittää langaton verkkoliikenne muihin kotiverkon laitteisiin ja vielä tärkeämmin internetiin. Turvallisessa verkossa vain sallitut laitteet voivat kytkeytyä tukiaseman tarjoamaan langattomaan verkkoon.

- Client-laitteet eli tietokoneet, puhelimet, pelikonsolit ja kodin erilaiset IoT laitteet kuten vaikkapa sääasema

- Router eli suomeksi reititin. Tämä on useimmiten yksi ja sama laite tukiaseman kanssa mutta tietoturvan kannalta on hyvä huomata, että se on erillinen toiminto.

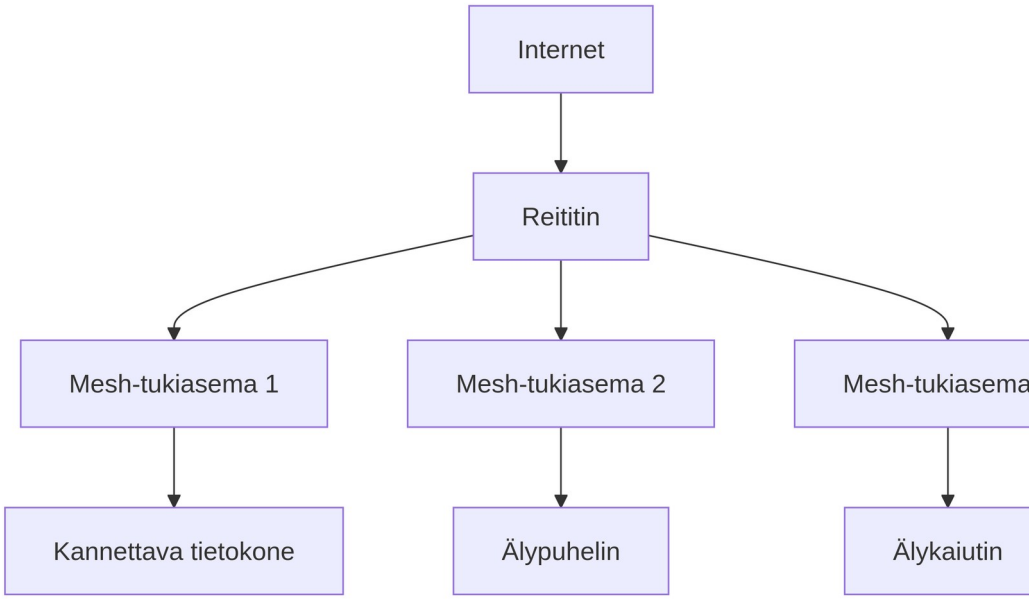
- Modeemi. Tämä vähän vanhahtava termi viittaa päätelaitteeseen johon reititin kytkeytyy jotta yhteys internetiin saadaan aikaan. Tänä päivänä yleisimpiä modeemityyppejä ovat 4/5G modeemit, kuitumodeemit ja jossain tapauksissa myös ADSL modeemit.(9,10)

Kotiympäristön langattomissa verkoissa on käytännössä useimmiten käytössä verkkotopologiana niin kutsuttu infrastruktuuritila jossa käytännössä koko verkko rakentuu yhden tai useamman reitittimen varaan. Toinen mahdollinen verkkotopologia WLAN verkoissa olisi niin kutsuttu Ad-hoc-tila eli toiselta nimeltään peer-to-peer tila jossa päätelaitteet muodostavat verkon itsenäisesti keskenään neuvottelemalla kahdenvälisiä yhteyksiä. Tällaiset verkot ovat varsinkin kotikäytössä erittäin harvinaisia.(9)

WiFi verkoissa liikenne perustuu lähetyspaketeihin joita on usean tyyppisiä mutta kaikissa paketeissa on niin sanottu header-osa eli otsikkotietue joka on joltain osin aina salaamaton. Otsikkotietueessa kulkee mukana mm. olennaisimmat tiedot siitä mikä verkko, keneltä ja kenelle paketti on matkalla. Näihin tietoihin liittyvät mm. SSID ja BSSID tunnukset.(11)

- SSID-kenttä (Service Set Identifier) sisältää yksinkertaisesti verkon nimen.(11)

- BSSID-kenttä (Basic Service Set Identifier) on uniikki tunniste jolla saman verkon reitittimet erottautuvat toisistaan. Toisinaan kentästä käytetään myös sen toista nimeä eli MAC-osoite (Media Access Control) (11)



Kuva 1. MESH-verkon toimintaperiaate

WiFi standardi on versioitunut vuosien varrella voimakkaasti. Tällä hetkellä uusin standardin saatavilla oleva versio on 7 joka esiteltiin vuonna 2024. WiFi standardi määrittelee monen muun asian lisäksi myös sen mitä taajuuksia käytetään ja mitä kanavia taajuuksilla voidaan käyttää. Lisäksi se sisältää maakohtaisia määrityksiä sillä kaikkia mahdollisia kanavia ei voida kaikkialla käyttää, koska niiden käyttämät taajuudet on varattu esimerkiksi tutka- tai muuhun käyttöön. Yleisimmin puhutaan 2.4GHz, 5GHz ja 6GHz verkoista. Vain uusimmat protokollaversiot tukevat 6GHz verkkoja ja niinpä niitä ei juuri kotiympäristöissä vielä olekaan. Toisaalta useimmat päätelaitteet tukevat myös vain 2.4GHz ja 5GHz verkkoja.(12)

Viime vuosina kotiympäristöissä ovat yleistyneet myös niin kutsutut MESH verkot. Näissä verkko rakentuu useammasta keskenään langattomasti keskustelevasta tukiasemasta. Näin kodin langaton verkko saadaan kattamaan paremmin koko kodin tila ja usein myös piha-alue. Ajatuksena on, että kukin MESH-tukiasema on niin lähellä seuraavaa, että muodostuva verkko on vahva

kaikkialla. Kyberturvan kannalta MESH-verkko ei yleisesti ottaen ole paras ratkaisu. Verkkotopologia altistaa avoimuutensa ansiosta koko verkon erityyppisille hyökkäyksille.(13,14)

Tärkeä kyberturvaominaisuus monissa nykyaikaisissa kotireitittimissä on tuki niin kutsutuille virtuaaliverkoille. Tallaisessa tapauksessa verkko näyttäytyy useammalla eri SSID:llä jolloin kotona voi olla vaikkapa erillinen vierasverkko johon vieraat voivat kytkeytyä ilman, että varsinaisen verkon turvallisuus vaarantuu.(9)

2.2 Yleisimmät uhat kotiverkoissa

Yleisimmin kotiverkkojen kyberturvapuutteet johtuvat pitkälti siitä, että niitä rakentaa ja ylläpitää maallikot joilla ei ole riittävää osaamistasoa, koulutusta eikä oikein aina kiinnostustakaan ymmärtää ja hallita reitittimen monimutkaisia asetuksia. Tämä johtaa helposti ongelmiin ja riskeihin joista ei edes olla tietoisia. Moni käyttäjä on tyytyväinen kunhan data liikkuu ja yhteyden nopeus on kyllin hyvä käyttäjän tarpeisiin. Kaiken lisäksi aivan liian usein reititin otetaan käyttöön oletusasetuksin jopa salasanaa vaihtamatta. Tämän lisäksi monien reititinten oletusasetukset eivät ole kyberturvallisia. Takavuosina saattoi jopa olla niin, että verkon oletusnimi ja oletussalasana olivat kaikissa valmistajan laitteissa sama. Siinä ei hyökkääjän tarvitse paljoa Google-hakua enempää tiedustelua tehdä saadakseen pääsyn verkkoon. Kun taitotaso on heikko tai välttävä ja laitteen oletusasetukset altistavat hyökkäyksille ei käyttäjä välttämättä edes huomaa joutuneensa hyökkäyksen tai haittaohjelman uhriksi. (15,16)

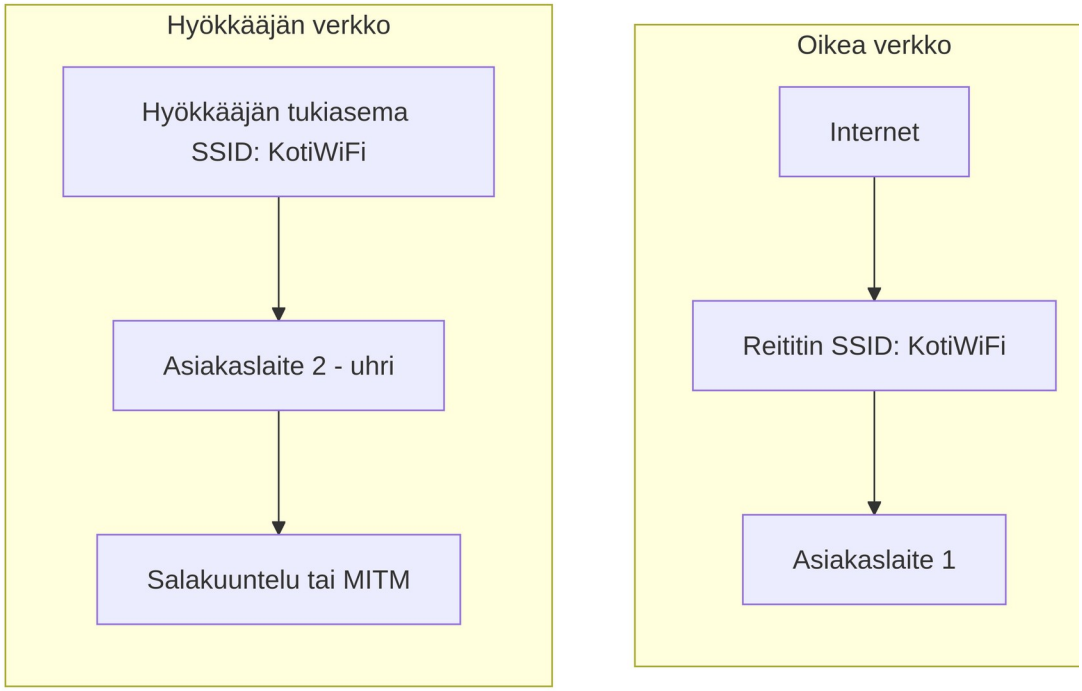
Vaikka uudemmat WiFi-standardin versiot ja sitä tukevat reitittimet ovatkin turvallisempia kuin aikaisemmin hälyyttävän usein kotiverkoissa edelleen löytyy joko niin vanhoja laitteita, ettei niissä ole esimerkiksi tukea uudemmille turvallisille salausmenetelmille tai käyttäjä ei osaa määrittää verkkoa oikein. Niinpä ei ole mitenkään erityisen epätavallista, että kotiverkko on joko kokonaan

avoin tai siinä on WEP-salaus. Avoimeen verkkoon pääsee kuka tahansa. Lisäksi WEP- ja WPA-salaukset on murrettavissa hyvin helposti. Jopa WPA2 on murrettavissa mikäli salasana on yksinkertainen tai löytyy sanahaulla. Vain uusin WPA3 on täysin turvallinen.(17,18)

Jo mainitsemani oletusasetusten käyttö on erittäin vaarallista sillä varsinkin yhdistettynä vanhaan tukiasemaan se saattaa johtaa siihen, että käyttäjällä on tunnettu tai muuten vaan huono salasana. Kaiken lisäksi moni tukiasema tarjoaa oletustasolla pääsyä myös asetusten määrityssivulle kaikille osoitteille. Osa jopa myös kiinteisiin ethernet yhteyksiin jolloin pääsy tukiaseman asetuksiin on pahimmillaan jopa kenelle tahansa internetissä. Mikäli myös hallintasivun salasana on asettamatta on tilanne hyvin pitkälti analoginen sen kanssa, että jättäisi kodin etuoven auki.(19)

Kaikilla laitteilla on suunniteltu käyttöikä. Tämä pätee myös reitittimiin. Valitettavasti tuo suunniteltukäyttöikä on usein paljon vähemmän kuin sen todellinen toimintakykyinen käyttöikä. Tällöin päädytään siihen, että laitevalmistaja lopettaa paikkausten ja korjausten toimittamisen vaikka laitekanta saattaa sinällään olla vielä täysin käyttökelpoista. Myös tämä johtaa helposti hyökkäyksille alttiisiin laitteisiin sillä kotikäyttäjän on varsin vaikea huomata päivitysten saatavuuden päättymistä – vaikka automaattiset päivitykset olisi kytketty päällekin.(20)

Kuva 1.



Kuva 2. Esimerkki Evil Twin tilanteesta. Kotikäyttäjä liittyy vahingossa väärään verkkoon

Kun pääsy verkkoon on saatu voidaan sitä käyttää monin eri tavoin. Usein monet kodin IoT laitteet on myös suojattu varsin huonosti. Näihin liittyvistä uhkaskenaarioista on paljon esimerkkejä takavuosilta. Yleisimmin laitteita pyritään kuitenkin keräämään ns. bottiverkkoihin joista niitä voidaan sitten käyttää hyökkäyksiin muualle ja tiedonkeruuseen.(21)

Moni tietämätön kotikäyttäjä saattaa asettaa itsensä vaaraan myös ihan hyvää hyvyyttään kun kodissa vierailee tuttu tai ystävä. Mikäli vieraita varten ei ole erikseen asetettu tai kodin verkkolaite ei tue ns. vierasverkko-toimintoa pääsee vierailevan henkilön päätelaite verkkoon kaikkian muiden kodin laitteiden kanssa. Jos vielä on niin ikävä tilanne, ettei reititin tue tai verkkosegmentointi ei ole päällä pääsee kenties saastunut vieraileva laite hyökkäämään kaikkiin kodin verkkolaitteisiin. (22)

Langattomiin verkkoihin liittyy myös tukku teknologioita jotka on alunperin tarkoitettu helpottamaan käyttöä mutta joista on myöhemmin muodostunut pikemminkin riesa käyttäjille. Tällaisia teknologioita ovat mm. WPS eli Wi-Fi Protected Setup sekä UPnP eli Universal Plug and Play. Molempien teknologioiden ajatus oli helpottaa laitteiden liittämistä langattomaan lähiverkkoon. Ikäväkyllä molemmat altistavat langattoman lähiverkon hyökkäyksille. UPnP protokollan murtaminen on triviaalia ja WPS murtuu mikälis siinä on niin kutsuttu PIN-kooditila päällä. (17)

Yllättävän tavallinen ongelma kotitalouksien langattomissa lähiverkoissa on myös reitittimen oletusnimen käyttäminen. Tällöin reitittimen nimi saattaa julkisesti näkyen olla esimerkiksi muotoa TeleWell500 tai NetgearNighthawk. Oletusnimen ongelma on se, että valmistajan lisäksi se sisältää myös tietoa tarkasta reititin mallista. Tätä tietoa voi jopa yksinkertaisella Google-haulla käyttää sen selvittämiseen, onko laitteella tunnettuja heikkouksia. Yleisiä nimiä on myös aavistuksen helpompi käyttää väärin joko ns. Evil Twin tai Honeypot hyökkäyksiin. Näissä hyökkäyksissä pyritään käyttäjä houkuttelemaan liittymään verkkoon houkuttelevan nimen perusteella. Kun käyttäjä verkkoon liittyy voidaan kaikkea käyttäjä verkkoliikennettä kuunnella.(23,24)

Kaiken kaikkiaan erilaiset uhat ja haavoittuvuudet ovat kotitalouksien langattomissa lähiverkoissa varsin yleisiä mutta usein turvatasoa olisi helppo nostaa yksinkertaisin keinoin. Tilanne ei siis ole toivoton.

2.3 Tietoturvan parhaita käytäntöjä

Ehdoton valtaosa kodin langattoman lähiverkon kyberturvaongelmista ja riskeistä on edelleen nykyäänkin vältettävissä ennalta ehkäisevällä varautumisella. Tämä tarkoittaa sitä, että langattoman lähiverkon asennus, määrittely ja ylläpito noudattaa parhaita kyberturvakäytäntöjä ja suoritetaan ajoissa. Ovet ikäänkuin lukitaan ennen kuin rosvo niitä kolkuttelee. Yleisesti ottaen tietoturvasuositukset tässä tutkimuksessa perustuu viranomaissuosituksiin kuten Kyberturvakeskuksen suosituksiin sekä

laitevalmistajien dokumentaatioon ja käytäntöihin. Tämän tutkimuksen tavoitteen on kerätä ja tuottaa sellaisia ohjeita ja parhaita käytäntöjä jotka ovat nimenomaan maallikon toteutettavissa ja onnistuvat tavalliselta käyttäjältä ilman kyberturvakoulutusta eikä vain asiantuntijoilta.(25)

Yleisesti ottaen langattoman lähiverkon turvallisuustason valinta lähtee liikkeelle oikean salausmenetelmän ja salaustason valinnalla. Tällöin kotikäyttäjän tulee välttää avoimia verkkoja. Ja valitun salauksen tulee olla riittävän vahva, ettei siinä ole tunnettuja haavoittuvuuksia tai, ettei sitä voida helposti murtaa. Tällöin kysymykseen tulee lähinnä WPA2 ja WPA3 salaukset. Mikäli kodin laitteet tukevat WPA3 salausta suositus olisi käyttää vain sitä sillä se on turvallisin saatavilla oleva langattoman lähiverkon salausprotokolla. Usein näin ei kuitenkaan ole. Tällöin valitaan joko WPA2+WPA3 tai WPA2-protokolla. Mikäli valittu salaus on WPA2 tai WPA2+WPA3 on tärkeää valita salasana siten, että se on kyllin vahva. WPA2 on mahdollista murtaa niin kutsutulla dictionary-attack hyökkäyksellä.(26,27)

Toinen tärkeä asia on laittaa hallintapaneelin näkyvyys pienelle ja varmistaa, että se on salasanalla suojattu. Lisäksi on tärkeää vaihtaa salasana. Kaikkein turvallisinta on mikäli hallintasivun saa kytkettyä näkyviin vain sisäverkon ethernet porttien kautta saatavalla yhteydellä. Tällöin hallintasivu ei ole lainkaan näkyvissä langattoman verkon laitteille. Myös mahdollinen etähallinta on parasta laittaa pois päältä. Etähallinnassa reititin on kaikenaikaa yhteydessä laitevalmistajan portaaliin internetissä. Tuo lisää hyökkäyspintaa tarpeettomasti. Myös verkkoon liittymistä helpottavat tekniikat WPS ja UPnP on syytä laittaa pois päältä jos mahdollista. Toisinaan WPS liitäntää ei saa kokonaan pois mutta tällöinkin on hyvä laittaa PIN-koodi liityntä pois päältä.(28,29)

Reitittimestä tulisi kytkeä automaattiset päivitykset päälle jotta mahdolliset haavoittuvuudet korjataan automaattisesti sitä mukaa kun laitevalmistaja niitä tarjoaa. Tämä on muuten syytä myös tehdä kaikille kodin verkkolaitteille mukaanlukien IoT-laitteet. Kun laitteen valmistaja lopettaa päivitysten

tarjoamisen on laite syytä kierrättää vaikka se muuten sinällään toimiva olisikin. Toki IoT laitteiden tapauksessa vaihtoehto voi myös olla kytkeä se pois verkosta jos laite muuten toimii hyvin.(20,30)

Mikäli langaton tukiasema toimintoa tukee on ehdottomasti hyvä laittaa verkkosegmentointi päälle ja luoda erillinen vierasverkko. Tällöin vieraat jotka hetkellisesti lainaavat verkkoa eivät pääse vahingossa saastuttamaan muuta verkkoa. Mikäli tukiasema tukee useita verkkoja jotka on mahdollista eristää toisistaan voi esim. pelikonsoleille ja IoT-laitteille myös luoda omat verkkonsa. Näin riskitaso esim. pankkitunnusten kalasteluun laskee entisestään kun ”puhtaassa” verkossa on vain suojattuja ja päivitettyjä laitteita.(22,9)

Langattoman verkon tukiaseman nimi on myös syytä vaihtaa siinäkin tapauksessa, ettei oletusnimi paljastaisi mitään olennaista tukiasemasta. Nimen tulisi helposti tunnistettavissa muttei mielellään myöskään sellainen, että siitä voi liian helposti päätellä omistajan nimen, osoitteen tai muuta olennaista. Aiemmin suositeltiin tukiaseman piilottamista mutta siitä on enemmän haittaa käyttäjälle kuin hyökkääjälle, joten piilottamista ei voi enää suositella. Neutraali vähän hajuton ja mauton nimi houkuttaa hyökkääjää kaikkein vähiten.(24,17)

Mikäli kodin langaton lähiverkko on rakennettu käyttäen MESH reitittimiä tulee varmistaa, että kaikilla verkon solmuilla asetukset on asetettu oikein salaustasoa, päivityksiä yms. myöten. MESH-verkkojen huono kyberturvataso johtuu useimmiten siitä, että yksi huonompi solmu riittää hyökkääjälle.(14,12)

Kun edellä olevaa listaa tarkastellaan, voidaan hyvin perusteella, että kodin langattoman lähiverkon ylläpitäjän tarkistuslista parhaisiin käytäntöihin on siis seuraava:

1. Vaihda oletusasetukset kuten tukiaseman nimi ja salasana, määrittelysivun näkyvyys ja salasana sekä tukiaseman nimi,

2. varmista riittävä salaustaso – vähintään WPA2 ja hyvä salasana,

3. muista automaattiset päivitykset,

4. käytä vierasverkkoja jos mahdollista,

5. Kytke pois WPS ja UPnP jos mahdollista ja

6. rajoita hallintasivun pääsy vain sisäverkkoon salasanalla suojaten.

3 Vaatimusmäärittely

Minkä tahansa ohjelmistoprojektin alkuvaiheena toimii yleensä aina vaatimusmäärittely. Se on myös eräällä tapaa koko projektin tärkein vaihe sillä se vaikuttaa suoraan saavutettavaan lopputulokseen. Vaatimusmäärittely rajaa mitä suunniteltu ohjelmisto tekee ja mitä se ei tee. Myös hyväksyntätestauksessa verrataan implementoituja ominaisuuksia vaatimusmäärittelyn asettamiin reunaehtoihin ja odotuksiin. Yllättävän usein on myös havaittavissa, että ongelmat ohjelmistoprojektin läpiviennissä ovat peräisin nimenomaan huonosti suoritetusta vaatimusmäärittelyvaiheesta.

Tässä projektissa vaatimusmäärittely keskittyy huomioimaan käyttäjien tarpeet sekä olennaisten kyberturvauhkien torjunta.

Kehitettävän sovelluksen kohdekäyttäjäkunta tässä tapauksessa on niin sanotut maallikkokotikäyttäjät jotka haluavat yksinkertaisen vastauksen kysymykseen: ”onko minun langaton lähiverkkoni turvallinen”? Työkalua on voitava käyttää missä tahansa vaiheessa kun verkko on olemassa. Kotikäyttäjälle helppo ratkaisu on mobiilisovellus joka on helppo asentaa ja suorittaa. Ammattilaisille on saatavilla suuri määrä työkaluja mutta ne ovat monimutkaisia ja vaikeita käyttää sekä vaativat suurta tietotaitotasoa.

Lisäksi on hyvä huomata, että tässä kohtaa rajaamme tavoitellun mobiilisovelluksen vain Android käyttöjärjestelmälle. Työkalun on myös tarkoitus testata nimenomaan langatonta lähiverkkoa ei esim. ethernet tms. verkkoa.

Tässä työssä vaatimusmäärittely on esitetty käyttäjätarinoina (User Stories), jotka perustuvat ketterässä ohjelmistokehityksessä, erityisesti Scrum-mallissa, käytettyyn dokumentointitapaan. Menetelmä mahdollistaa vaatimusten kuvaamisen loppukäyttäjän näkökulmasta selkeästi ja johdonmukaisesti. Vaatimukset on jaoteltu toiminnallisiin ja ei-toiminnallisiin, jotta voidaan erikseen kuvata, mitä sovellus tekee (toiminnallisuus) ja millä laatukriteereillä (ei-

toiminnallisuus) se toimii. Jaottelu tukee myös testauksen ja kehityksen suunnittelua.(31)

3.1 Toiminnalliset vaatimukset

Johdantolause: "Tässä kappaleessa esitetään sovelluksen keskeiset toiminnalliset vaatimukset käyttäjätarinoina (User Stories). Kukin tarina sisältää hyväksymiskriteerit (Acceptance Criteria), joiden täyttyessä toiminto katsotaan toteutetuksi vaatimuksen mukaisesti."

User Story 1: Verkkoanalyysin käynnistäminen
Käyttäjänä haluan aloittaa testin yhdellä painikkeella, jotta voin tarkistaa kotiverkkoni turvallisuuden helposti.
Hyväksymiskriteerit:

- Näytöllä on näkyvissä "Aloita testi" -painike
- Testi käynnistyy napista ja etenee vaiheittain
- Käyttäjä ei tarvitse teknistä osaamista

Heikosta salauksesta annetaan varoitus

User Story 2: Salaustyypin tunnistus
Käyttäjänä haluan nähdä, mitä salausta lähiverkkoni käyttää, jotta voin arvioida sen suojaustason.
Hyväksymiskriteerit:

- Salaustyyppi tunnistetaan (esim. WPA2, WPA3, WEP, avoin)
- Tuloksessa näytetään selkeä arvio (turvallinen / heikko)
- Heikosta salauksesta annetaan varoitus

User Story 3: WPS-tilan tarkastus
Käyttäjänä haluan tietää, onko WPS päällä, koska se voi heikentää tietoturvaa.
Hyväksymiskriteerit:

- WPS-status tunnistetaan automaattisesti
- Tila näytetään käyttäjälle tekstinä ja värein
- Jos WPS on päällä, näytetään varoitus

User Story 4: SSID-nimen analyysi
Käyttäjänä haluan tietää, onko verkon nimi oletusarvoinen tai tunnistettavissa, jotta voin vähentää hyökkäysriskiä.
Hyväksymiskriteerit:

- SSID verrataan tunnettuun oletusnimilistaan
- Jos nimi sisältää laitteen valmistajan nimen, annetaan huomautus
- Tuloksessa on suositus neutraalista nimestä

User Story 5: Rogue Access Point -tunnistus
Käyttäjänä haluan tietää, onko samalla SSID:llä useita tukiasemia, jotta voin havaita mahdolliset valeverkot.
Hyväksymiskriteerit:

- Sovellus listaa samannimiset verkot ja niiden BSSID:t
- Jos useita eri BSSID:iä havaitaan, annetaan huomautus

- Käyttäjä saa selityksen mahdollisesta “Evil Twin” -riskistä

User Story 6: CVE-haavoittuvuuksien tarkistus
Käyttäjänä haluan tietää, onko reitittimessä tunnettuja haavoittuvuuksia, jotta voin toimia ajoissa.
Hyväksymiskriteerit:

- BSSID tai SSID perusteella arvioidaan laitemalli
- CVE-tietokantaa käytetään vertailuun (esim. paikallisesti tai esikäsitelty lista)
- Haavoittuvuudet suodatetaan siten, että näytetään vain kriittiset paikkaamattomat haavoittuvuudet
- Haavoittuvuudet listataan selkeästi (nimi, vuosi, tyyppi)

User Story 8: Yhteenvedon ja riskianalyysin esittäminen
Käyttäjänä haluan nähdä koko testin lopputuloksen koosteena, jotta saan käsityksen verkkoni turvallisuustasosta.
Hyväksymiskriteerit:

- Kaikki yksittäiset testit listataan
- Tulokset näytetään väreillä (vihreä, keltainen, punainen)
- Koontiarvio (esim. "Verkko on melko turvallinen") esitetään selkeästi

User Story 9: Suositusten näyttäminen
Käyttäjänä haluan saada konkreettisia ohjeita, miten voin parantaa verkon turvallisuutta.
Hyväksymiskriteerit:

- Jokaiselle testille on siihen liittyvä suositus
- Suositukset näytetään vain, jos ongelma havaittiin
- Ohjeistus on selkokielinen ja käytännönläheinen

User Story 10: Oman kotiverkon tulosten erottelu ja tähtiluokitus
Käyttäjänä haluan nähdä oman kotiverkkoni tietoturvatulokset erillään muista verkoista ja saada sille selkeän 0–5 tähden arvosanan.
Hyväksymiskriteerit:

- Sovellus tunnistaa aktiivisen (yhdistetyn) verkon ja erottaa sen muista
- Tulokset näytetään omassa lohkossaan otsikolla "Kotiverkko" tai vastaavalla
- Kokonaisturvallisuudesta annetaan tähtiluokitus (0–5 tähteä)
- Tähtiluokitus perustuu painotettuun arvioon yksittäisten testien tuloksista

User Story 12: Muiden lähiverkkojen tulosten näyttäminen ilman luokitusta
Käyttäjänä haluan nähdä muiden alueella löytyvien Wi-Fi-verkkojen turvallisuustiedot, jotta voin vertailla tai tunnistaa mahdolliset riskiverkot.
Hyväksymiskriteerit:

- Sovellus listaa kaikki skannauksen aikana löytyneet verkot
- Jokaisesta näytetään esim. SSID, salaus, WPS-tila, oletusnimi jne.

- Näitä verkkoja ei arvostella tähdillä eikä nosteta esiin kuten omaa kotiverkkoa

- Näyttö toimii vertailuna ja mahdollistaa rogue-verkkojen tunnistamisen

3.2 Ei-toiminnalliset vaatimukset

Tässä kappaleessa esitetään sovellukselle asetetut ei-toiminnalliset vaatimukset käyttäjätarinoiden (User Stories) muodossa. Vaikka nämä vaatimukset eivät liity suoraan yksittäisiin toiminnallisiin ominaisuuksiin, ne määrittävät sovelluksen yleistä laatua, suorituskykyä, tietoturvaa ja käytettävyyttä. Jokaisen käyttäjätarinan yhteydessä on esitetty hyväksymiskriteerit, joiden täyttyminen osoittaa vaatimuksen täyttymisen. Näiden vaatimusten tarkoituksena on varmistaa, että sovellus on teknisesti luotettava, helppokäyttöinen ja soveltuu kohderyhmän tarpeisiin ilman ylimääräisiä järjestelmäriippuvuuksia tai turvallisuusriskejä.

User Story 13: Testien nopea suorittaminen
Käyttäjänä haluan, että sovelluksen suorittamat testit valmistuvat nopeasti, jotta en joudu odottamaan tuloksia kohtuuttoman pitkään.
Hyväksymiskriteerit:

- Kaikki testit suoritetaan tavallisella laitteella verrattain nopeasti

- Sovellus ei jäädy tai näytä epäaktiiviselta testin aikana ja antaa tietoa edistyksestä

- Käyttöliittymä näyttää etenemisen visuaalisesti

User Story 14: Yhteensopivuus Android-laitteiden kanssa
Käyttäjänä haluan, että sovellus toimii omalla Android-laitteellani ilman erityisiä järjestelmämuutoksia tai teknistä osaamista.
Hyväksymiskriteerit:

- Sovellus toimii vähintään Android 12.0 -versiossa tai uudemmissa
- Sovellus ei vaadi root-oikeuksia
- Sovellus käyttää vain käyttöjärjestelmän sallimia rajapintoja

User Story 15: Yksityisyyden säilyminen testauksen aikana
Käyttäjänä haluan, että sovellus ei jaa mitään tietoja ulkopuolisille, jotta voin käyttää sitä turvallisesti ja luottamuksellisesti.
Hyväksymiskriteerit:

- Sovellus ei lähetä Wi-Fi- tai laitetietoja verkkoon ilman lupaa
- Kaikki analyysi tapahtuu paikallisesti
- CVE-tietoja haetaan vain esikäsitellystä, laitteeseen tallennetusta tietokannasta tai anonyymisti

User Story 16: Selkeä ja saavutettava käyttöliittymä
Käyttäjänä haluan, että sovellus on helppokäyttöinen ja ymmärrettävä, jotta voin käyttää sitä ilman teknistä osaamista.
Hyväksymiskriteerit:

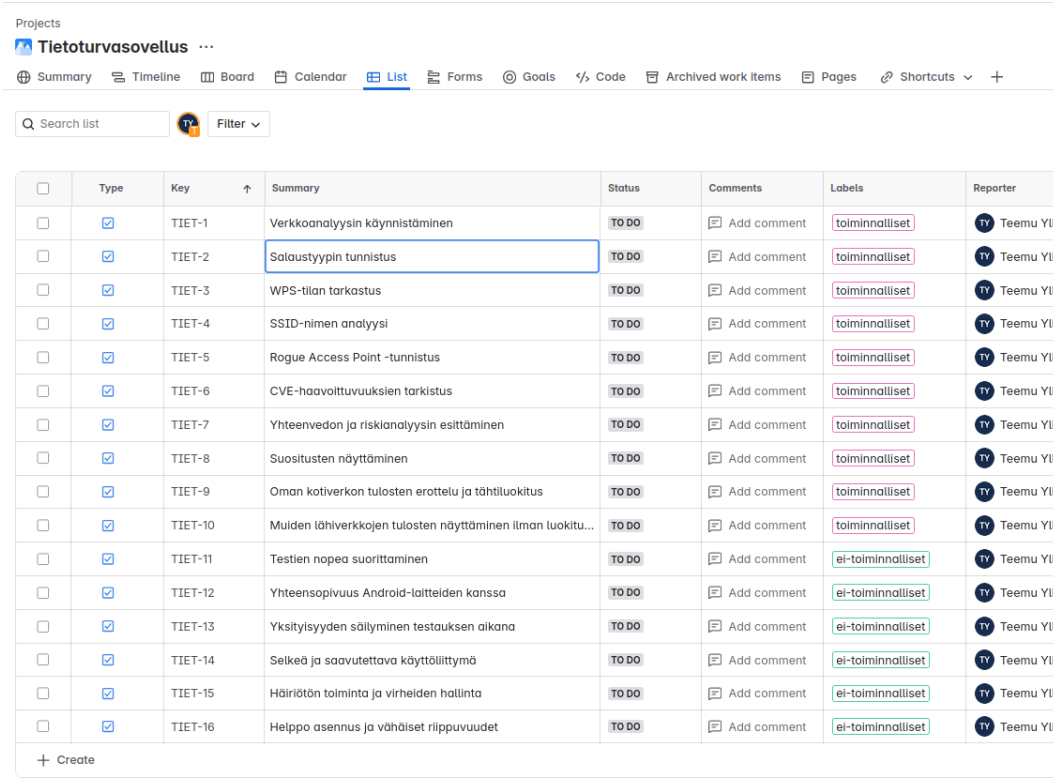
- Käyttöliittymä on selkeä ja looginen
- Tulokset esitetään värein ja tekstinä (ei pelkästään visuaalisin symbolein)
- Värit on valittu niin, että ne ovat ymmärrettävissä myös värisokeille

User Story 17: Häiriötön toiminta ja virheiden hallinta
Käyttäjänä haluan, että sovellus toimii luotettavasti ja ilmoittaa selkeästi, jos jokin testi epäonnistuu.
Hyväksymiskriteerit:

- Sovellus ei kaadu puuttuvien tietojen tai virhetilanteiden vuoksi
- Jos jokin testi ei onnistu (esim. WPS-tarkistus epäonnistuu), siitä näytetään virheilmoitus tai virhetilanne käsitellään muuten järkevästi

User Story 18: Helppo asennus ja vähäiset riippuvuudet
Käyttäjänä haluan, että sovelluksen voi asentaa helposti ilman ulkopuolisia kirjastoja tai lisäasetuksia, jotta käyttöönotto olisi vaivatonta.
Hyväksymiskriteerit:

- Sovellus toimii heti APK-asennuksen jälkeen
- Sovellus ei vaadi ulkoisia kirjastoja, joita ei sisällytetä julkaisuun
- Käyttäjän tarvitsee hyväksyä vain Wi-Fi-tiedon käyttöoikeus



Kuva 3. Sovelluksen kehitystä varten luotiin Jira-projekti

3.3 Jira Projekti

Sovelluksen projektinhallintaa ja työlistojen hallintaa varten valittiin käyttöön Atlassianin tarjoama Jira Cloud. Jira on laajasti käytetty projektinhallinta- ja seurantaohjelmisto, joka tukee erityisesti Scrum- ja Kanban-tyyppistä ketterää ohjelmistokehitystä. Sen avulla voidaan hallita ohjelmistokehitysprosessia käyttäjätarinoiden, tehtävien, vikojen ja muiden työyksiköiden kautta helposti seurattavassa muodossa.

Vaikka tässä työssä kehitystiimi koostui vain yhdestä henkilöstä, ketterien menetelmien mukainen työn osittaminen ja visuaalinen etenemisen seuranta katsottiin hyödylliseksi. Työn hallinta Jira-ympäristössä mahdollisti myös suoran sidonnan määriteltyihin käyttäjätarinoihin, jolloin vaatimukset, toteutus ja testaus liittyvät saumattomasti toisiinsa. Tämä lisää työn jäljitettävyyttä ja dokumentointia.

Käytännön tasolla kukin kappaleessa 3.1 määritelty käyttäjätarina (User Story) luotiin Jiraan omaksi työtehtäväksi (Issue type: Story) projektiin nimeltä Tietoturvasovellus. Tiketteihin liitettiin tunnisteet (label) jotka erottelivat toiminnalliset ja ei-toiminnalliset vaatimukset. Projektissa käytettiin Scrum-näkymää ja backlog-toiminnallisuutta, jotta työvaiheita voitiin järjestää kehitysvaiheittain. Kuvassa X esitetään otos backlog-näkymästä, jossa näkyvät vaatimusten mukaiset käyttäjätarinat tiketteinä.

Jira mahdollisti näin selkeän rakenteen ja toiminnallisuuden seuraamisen koko kehitystyön ajan. Se toimi samalla dokumentointityökaluna, jota voidaan hyödyntää myös testauksen ja arvioinnin vaiheessa.

4 Tekninen ympäristö

Kehitysympäristön, työkalujen, käytetyn ohjelmointikielen ja ulkoisten kirjastojen valinta määrittää pitkälti tuotetun sovelluksen kyvykkyyksiä sekä sovelluksen kompleksisuutta, tehokkuutta ja onpa sillä vaikutus myös implementointiin kuluvaan aikaan. Huonosti valittu kehitysympäristö voi johtaa huonosti toimivaan sovellukseen jota on vaikea ylläpitää ja kehitykseen käytetty aika venyy kohtuuttoman pitkäksi. Niinpä onkin tärkeää panostaa teknisen ympäristön määrittelyyn sen vaatimalla vakavuudella.

Moni teknisen ympäristön valintaan vaikuttavasta reunaehdosta lähtee jo määrittellyistä käyttäjätarinoista. Sovelluksen tulee toimia Android-laitteissa ilman root-oikeuksia (ks. User Story 14), käsitellä tietoja paikallisesti ilman ulkoista tiedonsiirtoa (User Story 15), ja olla käytettävissä myös offline-tilassa (User Story 17). Käytettävyyden ja selkeän käyttöliittymän tukemiseksi valittiin Flutter-kehys (User Story 16), joka myös mahdollistaa monialustaisen kehityksen myöhemmin, mikäli sovellus päätetään julkaista iOS-alustalle[1].

4.1 Käytetyt työkalut ja kirjastot

Käytettyjen työkalujen ja kirjastojen valinta lähtee ohjelmointikielen valinnasta. Tämän sovelluksen kehitykseen käytettäväksi kieleksi valikoitui Dart joka yhdistettynä Flutter SDK kehitysympäristöön tarjoaa modernin monialustakehitystä tukevan ympäristön jolla on helppo toteuttaa monipuolisia käyttöliittymiä ja jolle löytyy loistava Android tuki. Flutter käytännössä vaatii koneelle asennettuna myös Android Studion, Android SDK:n sekä laite-emulaattorin. Koodin kirjoittamiseen valikoitui Visual StudioCode joka on yleisesti käytetty ja varsin kevyt modulaarinen työkalu. (33,34,35)

Testilaitteiksi valikoin uudehkoja Android 12-15 käyttöjärjestelmällä varustettuja puhelimia.

[1] Tällä hetkellä iOS-käyttöjärjestelmä ei mahdollista kaiken tarvittavan tiedon noutoa mutta tilanteen muuttuessa tuki on mahdollista implementoida.

4.2 Kohdealusta ja tekniset rajaukset

Tämän insinöörityön puitteissa suunnitellun sovelluksen on tarkoitus toimia vain Android-laitteilla. IOS-käyttöjärjestelmän tukeen varaudutaan valikoimalla monialustateknologiaa tukeva kieli mutta tässä kohtaa rajaus on nimenomaan Android-laitteet. Toinen merkittävä rajaus on, että sovelluksen tulee toimia tavallisella laitteella ilman nk. root-oikeuksia. Erityisistä käyttöoikeuksista olennaisin on oikeus WiFi-dataan sekä pääsy internetiin jotta hakuja mm. CVE-tietokantaan voidaan tehdä. Sovellukset tulee toimia uudehkoilla laitteilla. Suunniteltu rajaus on vähintään Android 12 mutta siitäkin voidaan joustaa mikäli tekniset syyt niin edellyttää. Mitään erillistä ulkoista back-end palvelua ei ole tarkoitus tuottaa.(36)

5 Sovelluksen arkkitehtuuri

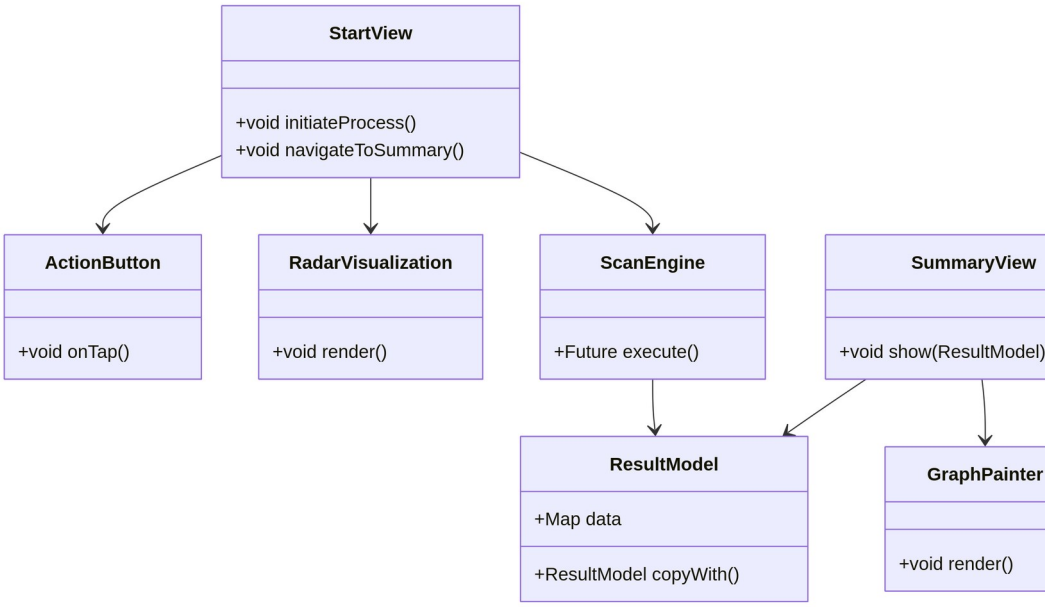
Yleisesti ottaen sovelluksen suunnittelu tulee aloittaa arkkitehtuuri-suunnittelusta. Valitsemalla tehtävään ja tekniseen ympäristöön soveltuva arkkitehtuuri voidaan sovelluksen kehitykseen käytettyä työaikaa säästää ja varmistetaan sovelluksen lähdekoodin eheys ja onnistunut kapselointi (37). Samalla voidaan kartoittaa tarvittavat suunnittelumallit. Oikein suunniteltu suunnittelumallienkäyttö varmistaa, että sovelluksen kehityksessä tehdyt tekniset ratkaisut ovat ominaisuuksiltaan tunnettuja. Näin pyritään myös välttämään niin kutsuttua spaghetti-koodia jonka ylläpito on hankalaa ja altista virheille. (38,39)

5.1 Korkean tason rakenne

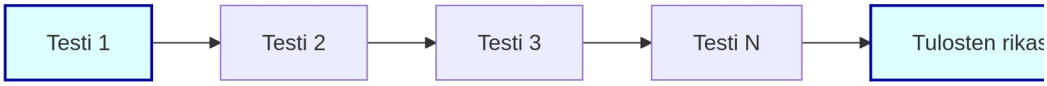
Tässä kappaleessa kuvataan sovelluksen korkean tason rakenne ja keskeiset luokkakomponentit. Kuvassa 4 seuraavalla sivulla oleva luokkakaavio esittää sovelluksen pääasialliset näkymät, tietorakenteet ja niiden väliset suhteet.

Sovellus käynnistyy StartView-näkymästä, jossa käyttäjälle esitetään aloituspainike ja visuaalinen odotusanimaatio. Kun käyttäjä aloittaa testauksen, StartView kutsuu ScanEngine-luokkaa, johon on kapseloitu eri testifunktiot, kuten salauksen tarkistus, WPS-tilan tarkistus ja CVE-tietojen haku. Testien tulokset kerätään tietorakenteeseen.

Kun testit on suoritettu, sovellus siirtyy SummaryView-näkymään, jossa ResultModel-luokan sisältö esitetään käyttäjälle luokiteltuna ja analysoituna raporttina sekä esitetään spektrinäkymä. Luokkien välinen rakenne tukee kapselointia, selkeyttää sovelluksen rakennetta ja helpottaa testattavuutta ja laajennettavuutta.



Kuva 4. Sovelluksen arkkitehtuuri



Kuva 5. Tietojarikastavan testiketjun toimintaperiaate

Sovelluksessa testausprosessin toteutukseen valittiin vaiheittainen analyysimalli, jossa yksittäiset testit muodostavat toisiaan seuraavan käsittelyketjun. Mallissa kukin vaihe vastaanottaa edellisen vaiheen tuottaman analyysitiedon, täydentää sitä omalla osuudellaan ja siirtää edelleen seuraavalle vaiheelle. Näin testitulokset rakentuvat kerroksittain, mahdollistaen tiedon rikastamisen ja eri näkökulmista tehtävän arvioinnin ilman tarpeetonta päällekkäisyyttä. Esimerkiksi salauksen tarkistus voi toimia perustana, jonka

päälle lisätään haavoittuvuustietoja, verkon ominaisuuksiin liittyviä havaintoja sekä muita turvallisuuteen liittyviä arvioita. Malli mahdollistaa laajennettavuuden ja tehokkaan tiedon hallinnan.

Tämä rakenne tuo useita hyötyjä sovelluksen toteutuksen ja ylläpidon näkökulmasta:

- Modulaarisuus: Jokainen testi toimii itsenäisenä ja selkeärajaisena komponenttina, joka ei ole riippuvainen testiketjun muista vaiheista.

- Laajennettavuus: Uusia testivaiheita voidaan lisätä ketjun loppuun ilman, että aiempien vaiheiden logiikkaa tarvitsee muuttaa. Tämä tukee myös jatkuvaa kehitystä ja uusien tietoturvaominaisuuksien tuomista mukaan.

- Jäljitettävyys: Tulos kumuloituu ja jokaisen testin vaikutus voidaan havaita erikseen. Tämä helpottaa virheiden paikantamista ja raportointia.

- Vältytään redundanssilta: Samoja verkko- ja laitteen tietoja ei haeta tai analysoida useaan kertaan eri vaiheissa, mikä parantaa suorituskykyä erityisesti resurssirajoitteisissa mobiililaitteissa.

- Yhteensopivuus funktionaalisten periaatteiden kanssa: Testivaiheet eivät muuta alkuperäisiä olioita vaan palauttavat muokattuja kopioita. Tämä lisää ohjelman ennustettavuutta ja testattavuutta.

Mallin soveltaminen on erityisen hyödyllistä tilanteessa, jossa analyysi perustuu osittain heuristiikkaan ja kerroksittaiseen päätöksentekoon. Transformation pipeline -mallia suositellaan yleisesti tällaisiin tilanteisiin, kuten esimerkiksi Fowler (2018) esittää refaktoroinnin ja funktionaalisen arkkitehtuurin yhteydessä.

5.2 Tietomalli

Sovellus on varsin yksinkertainen jossa on käytännössä kaksi näkymää ja testimoottori. Tästä syystä myös sovelluksen tietorakenne on pidetty yksinkertaisena. Tietorakenteeseen tallennetaan kaikki testien aikana keräillyt tulokset. Se toimii siis datankantajaelementtinä yksittäisten ketjutettujen testien välillä koko analyysin ajan. Tietomallin luokka on mutatoitumaton luokka. Käytännössä tällä varmistetaan, ettei tietue pääse korruptoitumaan testien välillä ja tästä syystä kukin testimetodi luo uuden instanssin kustakin tuloksesta käytten edellisen testin tuloksia. Näin syntyy aiemmin mainittu kumuloituva tuloksia rikastava testiputki.

ResultModel-luokan toiminnan kannalta olennaisia metodeita ovat copyWith() ja toString() -funktiot. Edellisellä luodaan uusi mutatoitumaton instanssi luokasta. Tämä on tärkeä osa ketjutusta. Jälkimmäisellä taas muutetaan numeerista tietoa tekstimuotoon jotta se voidaan esittää käyttäjälle ystävällisemmässä muodossa.

Tietomalli pitää sisällään useita eri kenttiä ja ne on mahdollista ryhmitellä mm. seuraavasti:

- Perustiedot: Nämä ovat kunkin reitittimen saatavilla olevia perustietoja. Jo tästä voidaan esimerkiksi salaustaso päätellä suoraan ilman suurempaa heuristiikkaa.

- Analyysitulokset: Nämä ovat syvempiä analyysituloksia jotka edellyttävät enemmän heuristiikkaa.

- Reititin- ja yhteystiedot: Näitä tietoja yhdistää tiedon julkisuus. Analyysi ei vaadi monimutkaista heuristiikkaa mutta tuloksia ei voi lukea suoraan WiFi-otsikkotiedoista.

- Kanavadata: Kanavadataan keräillään tieto kanavista jotta voidaan arvioida onko reititin määritelty käyttämään mahdollisimman vähäruuhkaista kanavaa.

- Yleinen huomautuskenttä: tietoturvaInfo. Tietorakenteeseen on myös varattu vapaampi tekstikenttä johon voidaan keräillä tekstuaalista dataa läpi koko testiputken. Esimerkiksi CVE-hakujen tiedot ovat juuri tällaista dataa.

5.3 Tietoturvatestien toteutus

Tietoturvatestit ovat koko sovelluksen keskiössä. Niiden onnistunut toteutus vaikuttaa sovelluksen toimintaan ja tulosten luotettavuuteen. Olemme rajanneet käyttäjäryhmän kotikäyttäjiin joten tulosten on oltava selkeitä ja luotettavia mutta toisaalta ammattikäyttöön tarkoitettujen työkalujen tarkkuusedellytys ei tässä käyttötarkoituksessa palevele tarkoitusta. Suunniteltu funktionaalinen ketjutettu testiputki mahdollistaa myös helpon jatkokehityksen kun testejä voidaan joustavasti lisätä putken jatkoksi sitä mukaa kun tarpeita tulee.

Testit hyödyntävät laitteen saatavilla olevia tietoja ja valittuja heuristisia sääntöjä, joiden perusteella arvioidaan mahdollisia riskejä. Näihin kuuluvat mm. salauksen vahvuus, oletusnimien käyttö, sekä viitteet epäilyttävistä verkoista.

Salaustason tunnistus

Perustasolla salaustason tunnistus on skannattujen WLAN-verkkojen perusteella varsin helppo arvioida. Yksinkertaisella haulla voidaan tunnistaa mitä salausprotokollaa reititin kertoo tukevansa. Tämän perusteella voidaan käyttäjälle antaa suositus käyttää tehokasta salausta.

WPS-tuen arviointi

Myös WPS tuki on helposti tutkittavissa. Mikäli WPS tuki on päällä reititin kertoo siitä. Tämä on siis mahdollista parsia yksinkertaisella tekstihaulla.

CVE-haavoittuvuusanalyysi

Kotikäyttäjän kannalta tärkeä tieto on mikäli käytössä olevalla reitittimellä on tunnettuja haavoittuvuuksia. CVE-hakuihin (Common Vulnerabilities and Exposures) sovellus käyttää Yhdysvaltain kauppaministeriön alaisen NIST:n virallista NVD (National Vulnerability Database) -tietokantaa johon on tarjolla avoin rajapinta. Mahdollisia laitehaavoittuvuuksia arvioidaan vertaamalla laitetietoja CVE-tietokannan esikäsiteltyyn otokseen.

Hallintasivun tunnistus

Hallintasivun tulisi olla suojattu jotta vierailijat, saastuneet laitteet, tms. eivät pääse muuttamaan verkon asetuksia. Mikäli hallintasivu löytyy annetaan varoitus.

SSID-oletusnimitarkistus

Oletusnimen tarkistaminen sinällään on varsin helppoa. Tämän jälkeen käytämme muodostettua listaa tunnetuista nimistä ja verrataan löytyykö nimestä komponentteja jotka muistuttavat tunnettuja oletusnimiä. Jos löydöksiä tehdään annetaan varoitus.

Kanavakuormitus ja -suositus

Käytetyn kanavan kuormitus on mahdollista laskea skannaustuloksista kun ne on keräilty tietomalliin. Tämän jälkeen kuormitus on käytännössä yhteenlaskuoperaatio. Paremman kanavan ehdottaminen perustuu siihen, että etsitään vapain kanava ja jos löytyy useita ehdotetaan ensimmäinen. Tämä logiikka voisi hyötyä jatkokehityksestä.

Rogue Access Point-tunnistus

Rogue accesspoint tilanne on yksi monista aktiivisen hyökkäyksen tilanteista. Tällöin verkkoon tuodaan tukiasemia, jotka pyrkivät hämäämään käyttäjää kirjautumaan väärään verkkoon jossa suojaus on ohitettu ja kaikkea käyttäjän liikennettä voidaan kuunnella. Mikäli tällainen tukiasema tunnistetaan annetaan varoitus.

Ad-hoc-verkkojen tunnistus

Toisinaan mahdollisen aktiivisen hyökkääjän tunnistaa siitä, että tukiasema itse kertoo olevansa ns. ad-hoc- eli tilapäisverkko. Mikäli tällainen verkko olisi käyttäjän käytössä ilman selkeää selitystä (esim. käyttäjä jakaa puhelimen verkkoa) on kyseessä mahdollisesti vaarallinen verkko. Tällöin annetaan varoitus.

MAC-spoofing-epäily

Toisinaan aktiivinen hyökkääjä käyttää laitetta joka luo suuren määrän virtuaalisia tukiasemia jotta tarjolla olisi useita hotspot verkkoja. Tällaisen tilanteen tunnistamiseen voidaan käyttää verkkojen valmistaja tietoa.Tietyt kuviot, kuten epätavallisen monet samanlaisten ominaisuuksien verkot, voivat viitata manipulointiin.

Vaaralliset SSID nimet

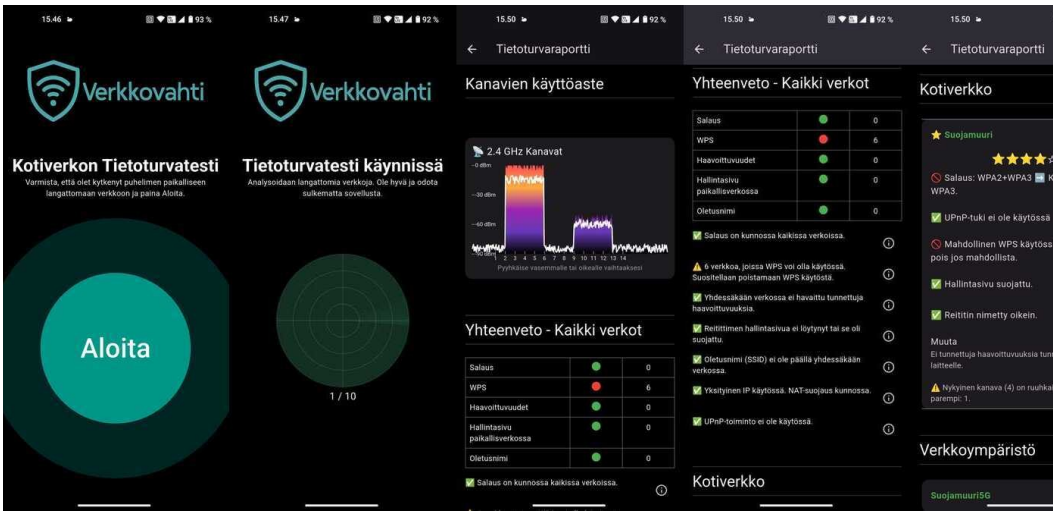
On olemassa laitteita jotka ovat tunnettuja hyökkäystyökaluja. Näiden tunnistukseen olen kerännyt listan, jota käytetään vertailuun. Mikäli laite tunnistetaan tällaiseksi annetaan varoitus käyttäjälle.

6 Käyttöliittymä

Verkkovahti-sovelluksen käyttöliittymä on suunniteltu selkeäksi ja helposti lähestyttäväksi myös vähemmän teknisille käyttäjille. Aloitusnäytöllä käyttäjää ohjeistetaan yhdistämään puhelin kotiverkkoon ennen testin aloittamista. Yksinkertainen ja suuri “Aloita”-painike käynnistää testin, jolloin käyttöliittymä siirtyy animaatioon perustuvaan testin etenemänäkymään. Animaatio tuo visuaalista palautetta testin etenemisestä ja kertoo käyttäjälle, että sovellus on aktiivinen.

Testin jälkeen käyttäjä saa tietoturvaraportin, jossa esitetään havainnot sekä visuaalisessa että taulukkomuodossa. Raportti näyttää muun muassa käytössä olevat kanavat, salauksen tilan, WPS-tuen olemassaolon ja reitittimen hallintasivun näkyvyyden. Kotiverkko nostetaan esiin erillisenä kokonaisuutena, jossa annetaan myös suosituksia tietoturvan parantamiseksi, kuten WPS:n poistaminen käytöstä tai vähemmän ruuhkaisen kanavan valitseminen.

Kokonaisuudessaan käyttöliittymä tukee sovelluksen päätarkoitusta: tarjota käyttäjälle helposti ymmärrettävää ja toimintaan ohjaavaa tietoa kotiverkon turvallisuudesta.



Kuva 6. Toteutetun sovelluksen käyttöliittymän näkymiä

7 Johtopäätökset ja jatkokehitys

Kokonaisuudessaan arvioiden projekti oli varsin onnistunut. Lopputuloksena todella syntyi mobiiliapplikaatio, joka tuottaa luotettavaa ja tarkkaa dataa käyttäjän langattomasta lähiverkkoympäristöstä. Tulokset on esitetty yhtenä raporttina, joka esittää kaiken kerätyn datan käyttäjälähtöisesti ja kertoo suositukset käyttäjälle. Sovellus antaa jopa tähti luokituksen käyttäjän omalle kotiverkolle joka kertoo yksinkertaisella mittarilla kuinka turvallinen verkko hänellä on. Jonkin verran kritiikkiä voisi esittää siitä, että varsinkin salaus, WPS ja UPnP asetuksia on yllättävän vaikea tavallisen käyttäjän säätää vaikka käyttäjälle annetaankin ohje. Sovelluksen raportissa on linkki kutakin testitulosta vastaavaan tietokorttiin jossa asetus ja sen käyttö pyritään selittämään yleiskielisesti. Tämä ei kuitenkaan ole kaikille riittävä sillä tukiasemien asetussivut ovat toisistaan hyvinkin suuresti poikkeavia. Toinen selkeä kritiikin lähde on tiedon paljous. Kun testejä on monta ja tukiasemia tyypillisesti kuitenkin ympärillä useita – joskus kymmeniä, tietoa kertyy raporttiin varsin paljon. Tämä saattaa hämätä joitakin käyttäjiä.

Testiyleisönä käytetyt henkilöt olivat varsin tyytyväisiä sovelluksen tuottamiin tuloksiin ja ne osoittautuivat varsin luotettaviksi.

Haastena sovelluksen implementoinnissa oli ehdottomasti tiedon vähyys ilman root-oikeuksia tai erillistä mittalaitetta. Toisaalta jo näillä mittareilla voidaan kotiverkkojen kyberturvaa parantaa huomattavasti.

Jatkokehityssuuntina on selkeästi havaittavissa tarve tiivistää tietoa ja esittää vain olennaista tietoa sekä auttaa käyttäjää asettamaan asetukset omassa reitittimessä oikein. Kuinka nämä tullaan toteuttamaan tulee vaatimaan lisätutkimuksia. Jatkokehityksessä voidaan tutkia mahdollisuutta hyödyntää verkon nimipalvelujen tai laitetunnisteiden analyysiä tarkempien arvioiden tuottamiseen. Testien jatkokehityksessä tulee myös seurata kehitystä. Mikäli uusia haavoittuvia teknologioita identifioidaan alalla tulisi niitä pyrkiä testaamaan. Ylläpito on tärkeä osa sovelluksen elinkaarta.

Vaikka työn tavoitteet saavutettiin suunnitellulla tavalla, joitakin rajoitteita jäi toteutukseen. Sovellus toimii teknisesti ilman root-oikeuksia, mutta tämä rajaa joidenkin syvällisempien analyysien toteuttamisen pois. Käyttöliittymä on selkeä, mutta ei välttämättä riittävä kaikille käyttäjäryhmille – erityisesti teknisesti vähemmän suuntautuneille. Toteutusvaiheessa käytetty tietorakenne osoittautui joustavaksi, mutta monimutkaisuus kasvoi ketjutetun analyysin myötä. Tulevaisuudessa keskittyisin enemmän laajempaan testaukseen eri laitteilla ja käyttäjäpalautteen keräämiseen kehitystyön tueksi.

Lähteet

1 Vodafone. *Home Wi-Fi usage increases as European households become more digital* [Internet]. Vodafone.com; 2022 Jun 16 [viitattu 2025 May 13]. Saatavilla: https://www.vodafone.com/news/products/home-wi-fi-usage-increases-as-european-households-become-more-digital

2 Cisco. *What is Wi-Fi?* [Internet]. Cisco.com; [päivämäärä ei saatavilla] [viitattu 2025 May 13]. Saatavilla: https://www.cisco.com/c/en/us/products/wireless/what-is-wifi.html

3 Laakso S. *Kotiverkkoasi voidaan käyttää vakoiluun – näin suojaudut* [Internet]. Verkkouutiset.fi; 2022 Oct 28 [viitattu 2025 May 13]. Saatavilla: https://www.verkkouutiset.fi/a/kotiverkkoasi-voidaan-kayttaa-vakoiluun-nain-suojaudut

4 Wi-Fi Protected Access. *Wikipedia* [Internet]. [viitattu 2025 May 13]. Saatavilla: https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

5 Wi-Fi Password Security - WEP, WPA, WPA2, WPA3. *CWNP* [Internet]. [viitattu 2025 May 13]. Saatavilla: https://www.cwnp.com/wifi-password-security/

6 Penetrating Networks by Cracking WPA 2. *DigForCE Lab* [Internet]. [viitattu 2025 May 13]. Saatavilla: https://blogs.dsu.edu/digforce/2023/07/11/penetrating-networks-by-cracking-wpa2/

7 Does WPA2/WPA3 mixed mode is less secure than pure WPA3? *Linus Tech Tips* [Internet]. [viitattu 2025 May 13]. Saatavilla: https://linustechtips.com/topic/1595234-does-wpa2wpa3-mixed-mode-is-less-secure-than-pure-wpa3/

8 WPA2 vs WPA3: Key Difference in Wi-Fi Security Protocols. *HFCL* [Internet]. [viitattu 2025 May 13]. Saatavilla: https://io.hfcl.com/blog/wpa2-vs-wpa3/

9 Cisco. What is Wi-Fi? [Internet]. Cisco.com; [date unknown] [cited 2025 May 13]. Available from: https://www.cisco.com/c/en/us/products/wireless/what-is-wifi.html

10 Wi-Fi Alliance. Wi-Fi CERTIFIED 7™ expands wireless performance for more demanding applications [Internet]. Wi-Fi.org; 2024 Jan 8 [cited 2025 May 17]. Available from: https://www.wi-fi.org/news-events/newsroom/wi-fi-certified-7-expands-wireless-performance

11 CWNP. Wi-Fi Packet Types [Internet]. CWNP.com; [cited 2025 May 17]. Available from: https://www.cwnp.com

12 TP-Link. What is a Mesh Wi-Fi System? [Internet]. TP-Link.com; [cited 2025 May 17]. Available from: https://www.tp-link.com/us/support/faq/1794

13 Netgear. What is the difference between a router, a modem, and an access point? [Internet]. Netgear.com; [cited 2025 May 17]. Available from: https://kb.netgear.com/23693

14 Linus Tech Tips. Mesh WiFi explained – and is it worth it? [Internet]. YouTube; 2022 [cited 2025 May 17]. Available from: https://www.youtube.com/watch?v=NgfY9j_wB94

15 CERT-FI. Suojaa langaton lähiverkkosi. Kyberturvallisuuskeskus [Internet]. [viitattu 2025 May 17]. Saatavilla: https://www.kyberturvallisuuskeskus.fi/fi/ohjeet-ja-oppaat/kansalaisille/suojaa-langaton-lahiverkkosi

16 ZDNet. The 10 most common Wi-Fi security mistakes [Internet]. [viitattu 2025 May 17]. Saatavilla: https://www.zdnet.com/article/the-10-most-common-wi-fi-security-mistakes/

17 CWNP. Wi-Fi Password Security - WEP, WPA, WPA2, WPA3 [Internet]. [viitattu 2025 May 17]. Saatavilla: https://www.cwnp.com/wifi-password-security/

18 DigForCE Lab. Penetrating Networks by Cracking WPA 2 [Internet]. [viitattu 2025 May 17]. Saatavilla: https://blogs.dsu.edu/digforce/2023/07/11/penetrating-networks-by-cracking-wpa2/

19 Shodan Blog. Default Passwords Are the Gift That Keeps on Giving [Internet]. [viitattu 2025 May 17]. Saatavilla: https://blog.shodan.io/default-passwords/

20 Ars Technica. Routers are still vulnerable long after support ends [Internet]. [viitattu 2025 May 17]. Saatavilla: https://arstechnica.com/gadgets/2022/08/router-vulnerabilities-persist-years-after-end-of-life/

21 Europol. Internet of Things (IoT) Security Report [Internet]. [viitattu 2025 May 17]. Saatavilla: https://www.europol.europa.eu/publications-documents/internet-of-things-security-report

22 TP-Link. How to set up Guest Network on your Wireless Router [Internet]. [viitattu 2025 May 17]. Saatavilla: https://www.tp-link.com/us/support/faq/837/

23 DEFCON. Attacking WiFi Protected Setup [Video]. DEFCON 20; 2012. Saatavilla: https://www.youtube.com/watch?v=RyL8T3yxq-I

24 Netgear. Best practices for WiFi SSID naming [Internet]. [viitattu 2025 May 17]. Saatavilla: https://kb.netgear.com/23494/

25 Kyberturvallisuuskeskus. Suojaa langaton lähiverkkosi – ohjeita kuluttajille [Internet]. Traficom.fi; [viitattu 2025 May 17]. Saatavilla: https://www.kyberturvallisuuskeskus.fi/fi/ohjeet-ja-oppaat/kansalaisille/suojaa-langaton-lahiverkkosi

26 CWNP. Wi-Fi Password Security - WEP, WPA, WPA2, WPA3 [Internet]. [viitattu 2025 May 17]. Saatavilla: https://www.cwnp.com/wifi-password-security/

27 HFCL. WPA2 vs WPA3: Key Difference in Wi-Fi Security Protocols [Internet]. [viitattu 2025 May 17]. Saatavilla: https://io.hfcl.com/blog/wpa2-vs-wpa3/

28 Shodan Blog. Default Passwords Are the Gift That Keeps on Giving [Internet]. [viitattu 2025 May 17]. Saatavilla: https://blog.shodan.io/default-passwords/

29 Linus Tech Tips. Is remote management on routers a security risk? [Video]. YouTube; 2023. Saatavilla: https://www.youtube.com/watch?v=w88Nop3TEII

30 Cisco. Internet of Things: Secure Your Devices [Internet]. [viitattu 2025 May 17]. Saatavilla: https://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html

31 Schwaber K, Sutherland J. *The Scrum Guide* [Internet]. Scrum.org; 2020 [viitattu 2025 May 17]. Saatavilla: https://scrumguides.org

32 Atlassian. *What is Jira Software?* [Internet]. Atlassian.com; [viitattu 2025 May 17]. Saatavilla: https://www.atlassian.com/software/jira

33 Google. Flutter – Build apps for any screen [Internet]. [viitattu 2025 May 17]. Saatavilla: https://flutter.dev/

34 Flutter documentation. Install – Android setup [Internet]. [viitattu 2025 May 17]. Saatavilla: https://docs.flutter.dev/get-started/install

35 Microsoft. Visual Studio Code – Code Editing. Redefined [Internet]. [viitattu 2025 May 17]. Saatavilla: https://code.visualstudio.com/

36 Android Developers. Manifest.permission documentation [Internet]. [viitattu 2025 May 17]. Saatavilla: https://developer.android.com/reference/android/Manifest.permission

37 Bass L, Clements P, Kazman R. *Software Architecture in Practice*. 3rd ed. Boston: Addison-Wesley; 2013.

38 Gamma E, Helm R, Johnson R, Vlissides J. *Design Patterns: Elements of Reusable Object-Oriented Software*. Boston: Addison-Wesley; 1995.

39 McConnell S. *Code Complete: A Practical Handbook of Software Construction*. 2nd ed. Redmond: Microsoft Press; 2004.

40 Fowler M. *Refactoring: Improving the Design of Existing Code*. 2nd ed. Boston: Addison-Wesley; 2018.

41 National Institute of Standards and Technology. National Vulnerability Database (NVD) [Internet]. Gaithersburg (MD): U.S. Department of Commerce; [cited 2025 May 17]. Available from: https://nvd.nist.gov

42 The MITRE Corporation. Common Vulnerabilities and Exposures (CVE) [Internet]. Bedford (MA): MITRE; [cited 2025 May 17]. Available from: https://cve.mitre.org

43 National Institute of Standards and Technology. National Vulnerability Database (NVD) [Internet]. Gaithersburg (MD): U.S. Department of Commerce; [cited 2025 May 17]. Available from: https://nvd.nist.gov