HAMK
Hämeen ammatti-
korkeakoulu

Internetiin yhteydessä olevien autojen kyberturvallisuus

Ammattikorkeakoulututkinnon opinnäytetyö

Tietojenkäsittelyn koulutus

Kevät 2024

Johannes Nikkanen

HAMK
Hämeen ammatti-
korkeakoulu

Tietojenkäsittelyn koulutus Tiivistelmä
Tekijä Johannes Nikkanen Vuosi 2024
Työn nimi Internetiin yhteydessä olevien autojen kyberturvallisuus
Ohjaaja Ismo Turve

Opinnäytetyön aiheena on internetiin yhdistettyjen autojen kyberturvallisuus. Työn tarkoituksena oli selvittää, millaisia kyberuhkia moderneihin, internetyhteydellä varustettuihin henkilöautoihin kohdistuu, ja miten autoteollisuus on reagoinut niihin. Myös autoilijan mahdollisuuksia vaikuttaa omaan kyberturvallisuuteensa tutkittiin.

Opinnäytetyö on tutkimuksellinen, ja siinä käytettyjä tutkimusmenetelmiä ovat kirjallisuuskatsaus sekä tapaustutkimus. Kirjallisuuskatsausta käytettiin opinnäytetyön tietoperustan kokoamiseen, ja tapaustutkimusta yhden henkilöauton kyberturvallisuusriskien kartoittamiseen.

Työn tietoperustassa tarkastellaan autojen digitalisaatiota sekä auton sisäisten että ulkoisten tiedonsiirtomenetelmien osalta, käydään läpi työn kannalta oleelliset kyberturvallisuuteen liittyvät käsitteet, sekä tarkastellaan autoihin liittyviä kyberuhkia ja niiden torjumiseksi käytettyjä menetelmiä. Tietoperustassa käsiteltyjen asioiden pohjalta toteutettiin myös riskikartoitus, joka koski yhden auton langattomia yhteyksiä käyttäviä järjestelmiä.

Tutkimuksessa havaittiin, että autoihin kohdistuu useita kyberuhkia, jotka vaihtelevat vakavuutensa suhteen melko laajasti. Kun tarkasteltiin uhkien torjumisen kehitystä, havaittiin, että sekä autojen valmistajat että lainsäätäjät ovat reagoineet uhkiin, ja kehittäneet toimintaansa ja sääntelyä kyberturvallisuuden kannalta positiiviseen suuntaan. Johtopäätöksenä voidaan todeta, että uusimmat autot ovat kyberturvallisuutensa suhteen hyvin suojattuja ulkoisten tahojen tekemiltä hyökkäyksiltä. Samaan aikaan autojen valmistajat pääsevät kuitenkin käsiksi yhä suurempaan määrään autoilijan dataa, mikä voidaan nähdä myös uhkana.

Avainsanat Kyberturvallisuus, CAN-väylä, henkilöauto, langaton tiedonsiirto
Sivut 38 sivua ja liitteitä 3 sivua

HAMK
Hämeen ammatti-
korkeakoulu

Degree Programme in Business Information Technology
Author Johannes Nikkanen
Subject Cybersecurity of cars with internet connection
Supervisors Ismo Turve

Abstract
Year 2024

The topic of this thesis is cybersecurity of cars with internet connection. The purpose was to find out, which kind of cyber security threats are related to modern, internet-connected cars, and how the automotive industry has reacted to the threats. Drivers' possibilities to affect their own cybersecurity were also researched.

The thesis is theoretical, and the research methods used were literature review and case study. The literature review was used to gather the information for theoretical background, and the case study was used to analyze the cyber risks of wireless systems in a specific car.

The theoretical background consists of information about the digitalization of cars, including their internal and external data-transfer systems. The relevant concepts of cyber security are also addressed, as well as the cyber threats and risks of cars and their mitigation methods.

The research demonstrates that there are multiple cyber threats concerning modern cars, which vary a lot considering their severity. While examining the evolution of the methods for preventing cyber threats, it was noted that automotive industry and legislators have both reacted to the threats and improved their actions and regulations. It can be stated as a conclusion, that the newest cars are quite safe considering the risks created by third-party threat actors. On the other hand, the manufacturers of the cars have access to increasing amount of data from the drivers, which can be considered a threat as well.

Keywords Cybersecurity, CAN bus, passenger car, wireless communication
Pages 38 pages and appendices 3 pages

Sanasto

ECU	Electronic Control Unit, elektroninen ohjainlaite
TCU	Telematics Control Unit, telematiikan ohjainlaite
CAN	Controller Area Network, tiedonsiirtoprotokolla, jota käytetään laajasti ajoneuvoissa
ISO	International Organization for Standardization, kansainvälinen standardoimisjärjestö
SAE	Society of Automotive Engineers, standardeja kehittävä ammattijärjestö
IEEE	Institute of Electrical and Electronics Engineers, sähkö- ja elektroniikkatekniikan standardeihin keskittyvä järjestö
UNECE	United Nations Economic Commission for Europe, YK:n Euroopan Talouskomissio
RKE	Remote Keyless Entry
PKE	Passive Keyless Entry
WLAN	Wireless Local Area Network, langaton lähiverkko
DSRC	Dedicated Short Range Communication, lyhyen kantaman tiedonsiirto

Sisällys

1 Johdanto 1
2 Tutkimuskysymykset ja -menetelmät 2
2.1 Tutkimuskysymykset 2
2.2 Tutkimusmenetelmät 2
3 Autoteollisuuden digitalisaatio 4
3.1 ECU 4
3.2 Perinteiset tiedonsiirtoväylät 5
3.2.1 CAN 5
3.2.2 FlexRay 6
3.2.3 MOST 6
3.3 Automotive Ethernet 7
3.4 Telematiikka 7
4 Autojen langattomat yhteydet 8
4.1 Bluetooth 8
4.2 Avaimeton kulku 8
4.2.1 RKE 8
4.2.2 PKE 9
4.3 Matkapuhelinverkko 9
4.4 Wi-Fi 9
4.5 DSRC 10
5 Kyberturvallisuus 11
6 Autoihin kohdistuvat kyberuhat ja -hyökkäykset 13
6.1 Tunnetut haavoittuvuudet 13
6.1.1 Fiat-Chrysler Uconnect 13
6.1.2 BMW ConnectedDrive 14
6.2 Uhkien kehitys 15
6.3 Hyökkäysskenaariot 16
6.3.1 Etäyhteydellä toteutettavat hyökkäykset 17
6.3.2 Lyhyen kantaman yhteyksiin kohdistuvat hyökkäykset 17
6.3.3 Fyysistä pääsyä edellyttävät hyökkäykset 18
7 Valmistajien tiedonkeruu 20
7.1 Tilanne Suomessa 20
7.2 Tiedonkeruun riskit 22
8 Turvallisuusprotokollat ja -ratkaisut 24

8.1 Päivitysmekanismit ja haavoittuvuuksien hallinta 24
8.2 Standardit ja sääntely 24
8.2.1 SAE J3061 25
8.2.2 ISO/SAE 21434 25
8.2.3 UNECE WP.29 R155 & R156 26
8.3 Salausmenetelmät 26
8.4 IDS 27
8.5 Avainten suojamekanismit 28
9 Riskien kartoittaminen ja CAN-viestinnän takaisinmallinnus 29
9.1 Riskienhallintaprosessi 29
9.2 Käytetyt työkalut ja ohjelmat 30
9.3 Auton järjestelmien riskikartoitus 30
9.4 CAN-viestien takaisinmallintaminen ja lähettäminen 32
10 Johtopäätökset ja pohdinta 35
10.1 Opinnäytetyöprosessi 35
10.2 Tulokset 36
11 Yhteenveto 38
Lähteet 39

Kuvat ja komennot

Komento 1, CAN-väylän datan tallentaminen tiedostoon 32

Komento 2, tiedoston tarkastelu komentoriviltä 33

Komento 3, tiedoston jakaminen puoliksi 33

Komento 4, tiedostojen lähettäminen CAN-väylään 33

Komento 5, ovet lukitsevan viestin lähettäminen 34

Komento 6, lukituksen avaavan viestin lähettäminen 34

Kuva 1, CAN-viestin rakenne 5

Kuva 2, FlexRay-hybriditopologia 6

Kuva 3, hyökkäysvektorien jakautuminen 16

Kuva 4, tunkeutumisen havaitsemisjärjestelmän toiminta Vectorin kuvaa mukaillen ... 28

Kuva 5, tallennetun tiedoston rakenne 33

Liitteet

Liite 1. Aineistonhallintasuunnitelma

Liite 2. Riskikartoitus

1 Johdanto

1900-luku oli nopean kehityksen aikaa. Autojen sarjatuotannon aloittaminen johti niiden saatavuuden nopeaan kasvuun, ja tietokoneet kehittyivät vuosisadan puolivälin jälkeen laskentatehon suhteen eksponentiaalisesti. Nykyisin Suomessa on lähes yhtä paljon henkilöautoja kuin ihmisiä, ja internet on kaikille saatavilla. 2010-luvulla nämä kaksi alun perin toisiinsa liittymätöntä asiaa kohtasivat, kun autojen valmistajat alkoivat yhdistää autojaan verkkoon.

Kehityksen myötä on syntynyt paljon hyvää, mutta myös uudenlaisia uhkia on muodostunut. Kyberrikollisuus on nopeasti kasvava rikollisuuden muoto, jolta mikään nettiin yhdistetty ei ole turvassa ilman asianmukaista suojausta. Myös verkon käyttäjien yksityisyydensuoja on herättänyt huolta, ja siihen on yritetty puuttua kehittämällä lainsäädäntöä ohjaamaan yritysten toimintaa. Kun verkkoyhteys löytyy miltei jokaisesta uudesta autosta, koskevat nämä uhat myös niiden käyttäjäkuntaa.

On arvioitu, että kyberrikollisuuden aiheuttamat kulut autoteollisuudelle voivat olla jopa yli 100 miljardia vuodessa (Upstream, 2023, s.51), joka varmasti motivoi autoteollisuuden toimijoita pohtimaan keinoja kyberturvallisuuden parantamiseksi.

Tässä opinnäytetyössä käyn läpi autojen digitalisaation kehitystä, ja selvitän autoihin kohdistuvien kyberuhkien kehitystä ja nykytilaa. Pyrin työssä löytämään vastaukset kysymyksiin siitä, miten autoteollisuus ja lainsäätäjät ovat reagoineet uhkiin, ja miten autoilija voi välttyä kyberrikollisuuden uhriksi joutumiselta.

Tässä tutkimuksessa etsitään vastauksia seuraaviin kysymyksiin:

-Millaisia uhkia internetiin yhteydessä oleviin autoihin kohdistuu?

-Miten uhkiin on reagoitu?

-Miten autoilija voi välttää tai torjua uhkia?

2 Tutkimuskysymykset ja -menetelmät

Tässä luvussa tutustutaan tarkemmin työn tutkimuskysymysten valinnan taustalla oleviin syihin ja menetelmiin, joita työn toteutuksessa käytetään.

2.1 Tutkimuskysymykset

Tutkimuskysymyksiä, joihin työssä pyrittiin vastaamaan, oli kolme. Niistä ensimmäinen, millaisia uhkia internetiin yhteydessä oleviin autoihin kohdistuu, oli selkeä valinta. Tiedossa olevien ja mahdollisten uhkien tarkastelu on tärkeä osa kokonaiskuvan muodostamista varten.

Kyberturvallisuuden kehittämiseksi tarvitaan erinäisiä toimenpiteitä, kuten järjestelmien koventamista ja sitä ohjaavaa lainsäädäntöä. Toinen tutkimuskysymys, miten uhkiin on reagoitu, jatkaa aiheen käsittelyä siitä, mihin ensimmäinen kysymys jäi. Siihen vastaamalla pystytään luomaan kuvaa tilanteen kehittymisestä ja myös hieman tulevaisuuden näkymistä.

Kolmas tutkimuskysymys, miten autoilija voi välttää tai torjua uhkia, käsittelee kyberturvallisuutta autoilijan näkökulmasta. Se on myös tärkeää, sillä loppukäyttäjä itse voi usein vaikuttaa toiminnallaan kyberturvallisuuteensa niin hyvässä kuin pahassa.

2.2 Tutkimusmenetelmät

Tärkeimpänä menetelmänä työn teossa oli kirjallisuuskatsaus. Kirjallisuuskatsauksen käytölle tutkimusmenetelmänä voi olla useita syitä, kuten uuden teorian rakentaminen ja arvioiminen tai kokonaiskuvan rakentaminen (Salminen, 2011, s.3). Tässä työssä merkittävin syy oli sen soveltuvuus kokonaiskuvan rakentamista varten.

Kirjallisuuskatsaukset voidaan jakaa karkeasti kolmeen pääryhmään, jotka ovat kuvaileva ja systemaattinen kirjallisuuskatsaus ja meta-analyysi. Tässä työssä käytettiin kuvailevaa kirjallisuuskatsausta, jota voidaan sanoa myös yleiskatsaukseksi sen suhteellisen vapaan muodon vuoksi. Sen tunnuspiirteenä on laajojen ja keskenään erilaisten aineistojen käyttö, joilla tutkittava ilmiö pystytään kuitenkin kuvaamaan riittävän laajasti. (Salminen, 2011, s.6)

Katsauksessa käytettyjen lähteiden etsimiseen käytettiin Google Scholaria, Hamk Finnaa ja Googlen hakua. Aineisto koostui mm. aihetta käsittelevistä tieteellisistä julkaisuista, nettijulkaisujen artikkeleista ja raporteista sekä kirjoista.

Työn käytännön osassa tutkimusmenetelmänä käytettiin tapaustutkimusta. Tapaustutkimuksessa tapaus tarkoittaa rajattua kokonaisuutta tai yksikköä, josta pyritään luomaan yksityiskohtaista tietoa. Tapauksia voi olla useampi kuin yksi, jolloin ne muodostavat yhdessä tutkimuskohteiden joukon. Tapaustutkimuksessa ei pyritä luomaan yleistävää tietoa, mutta sen tulokset ovat usein kuitenkin jollain lailla yleistettävissä. (JYU, 2015)

3 Autoteollisuuden digitalisaatio

Autoteollisuus otti ensimmäiset askeleensa kohti digitalisaatiota 1970-luvulla, kun elektroniset ohjainlaitteet, ECUt, joilla säädeltiin polttoineen sytytyksen ajoitusta, ilmestyivät GM:n ja Fordin sarjatuotantomalleihin.1980-luvulle tultaessa moottorinohjaus hoidettiin jo laajemmin tietokoneita hyödyntäen, ja autojen turvallisuusjärjestelmien, kuten lukkiutumattomien jarrujen tai luistoneston yleistyessä myös ohjainlaitteiden määrä kasvoi. (Mertl, 2016)

2010-luvun puolivälin uudessa autossa oli jo keskimäärin 25–50 ohjainlaitetta, joilla kontrolloitiin yhä useampia järjestelmiä ohjauksesta, kaasusta ja jarrusta alkaen. Tässä vaiheessa autoista alettiin puhumaan pyörillä kulkevina tietokoneina. (Mertl, 2016)

Samoihin aikoihin autoja alettiin varustaa myös entistä kehittyneemmillä, kosketusnäytöillä varustetuilla tietoviihdejärjestelmillä, joita voi ohjata myös puhekomennoilla. Samalla sensoreiden ja ohjainlaitteiden määrä jatkoi kasvuaan uusien turvallisuusjärjestelmien, kuten adaptiivisen vakionopeudensäätimen ja automaattisen hätäjarrujärjestelmän yleistymisen myötä. (Di Francesco, 2023)

Seuraavissa luvuissa kerrotaan tarkemmin ECUsta, esitellään autojen perinteiset sisäiseen tiedonsiirtoon käytetyt teknologiat ja Ethernetin käyttö autoissa, sekä käydään läpi mitä telematiikka on ja miten se liittyy moderneihin autoihin.

3.1 ECU

ECU (electronic control unit), eli elektroninen ohjainlaite, on pieni tietokone, joka koostuu useimmiten prosessorista, muistista, ja mikropiiristä. Se prosessoi siihen liitetyiltä sensoreilta saatua tietoa, ja suorittaa sen pohjalta sille määriteltyjä toimintoja, mutta voi myös lähettää tätä tietoa muille ECUille niiden toiminnan mahdollistamiseksi. (TechSparks, 2023)

ECUt on suunniteltu toimimaan huonoissakin olosuhteissa, ja niissä käytetään edistynyttä teknologiaa toimintahäiriöiden varalta (TechSparks, 2023). Kyberturvallisuutta niiden suunnittelussa ei kuitenkaan alun perin huomioitu lainkaan. Nykyisin viestintää ECUjen välillä on usein rajoitettu. (Borza, 2021)

3.2 Perinteiset tiedonsiirtoväylät

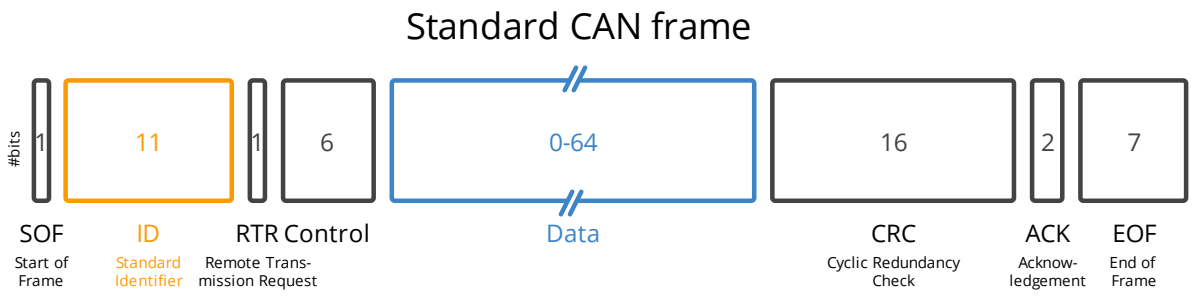
Nykyisin miltei jokaista auton komponenttia, jopa ajovaloja ja ovenkahvoja, ohjaa yksi tai useampi ECU. Jotta esimerkiksi nykyisin yleiset kaarreajovalot toimisivat, täytyy tieto ratin liikkeistä siirtyä valojen toimintaa säätelevälle ECUlle. Tämä on toteutettu autoissa yhdistämällä ohjainlaitteet auton sisäiseen verkkoon tai verkkoihin, jossa ne voivat siirtää tietoa keskenään. Tähän tarkoitukseen on käytetty viimeisten vuosikymmenten aikana useita teknologioita, joista tunnetuimpia ovat CAN-väylä, MOST ja FlexRay. (Knight, 2020, ss. xxiv–xxv) Näiden teknologioiden toiminnan ymmärtäminen on oleellista, jotta saadaan käsitys siitä, millaisia uhkia ne muodostavat ulkoisen verkkoyhteyden kanssa.

3.2.1 CAN

CAN (Controller Area Network) -väylä kehitettiin jo 1980-luvulla, ja nykyisin se on käytössä lähes kaikissa ajoneuvoissa. Järjestelmässä ohjainlaitteet on yhdistetty sähköjohtojen määrän minimoimiseksi CAN-väylään, johon ne lähettävät viestejä. Viestit välittyvät väylän kaikille muille ohjainlaitteille, jolloin laitteiden viestiminen keskenään mahdollistuu ilman ohjainlaitteiden kytkemistä suoraan toisiinsa. CAN-väylä on määritelty ISO:n (International Organization for Standardization) standardeissa, joista ISO 11898-1 ja ISO 11898-2 käsittelevät high speed CAN-väylän siirto- ja fyysistä kerrosta. (Falch, 2022)

Tavallisessa CAN-väylän viestissä on aina samanlainen rakenne. Se koostuu kahdeksasta osasta, jotka nähdään Kuva 1. Tärkeimpiä ovat tunniste- ja dataosat. Tunnisteen koko on 11 bittiä, ja se määrittää viestin tärkeyden. Mitä pienempi arvo tunnisteella on, sitä tärkeämpi viesti on, ja sitä nopeammin siihen reagoidaan. Data-kentässä on viestin tietosisältö, joka on kooltaan enintään 8 tavua eli 64 bittiä. Datan oikeellisuuden vahvistamiseksi käytössä on CRC (Cyclic Redundancy Check) -algoritmi. (Falch, 2022)

Kuva 1, CAN-viestin rakenne (Falch, 2022)



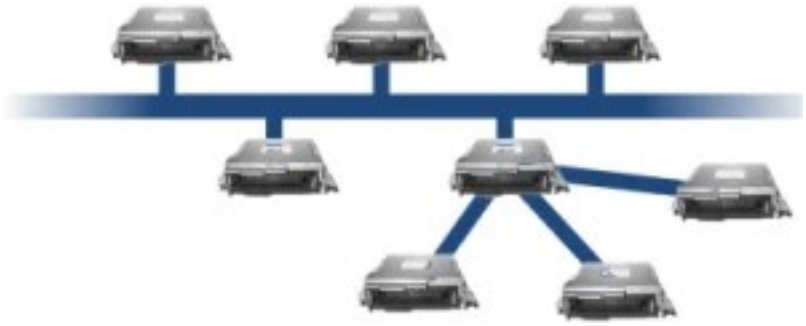
CAN-väylää ei itsessään ole suojattu millään tavalla, eikä siinä kulkevaa liikennettä ole salattu. Mahdollisesta suojauksesta huolehtiminen on jätetty autovalmistajan toimenpiteiden varaan. Tämä voi johtaa siihen, että väylään käsiksi pääsevä hyökkääjä pystyy syöttämään väylän ohjainlaitteille valheellista tietoa, ja siten vaikuttamaan niiden toimintaan. (Knight, 2020, s. xxvi) Helpoiten yhteyden CAN-väylään saa fyysisesti auton OBD2-diagnostiikkaportin kautta, joka on suoraan yhteydessä väylään. Se sijaitsee yleensä kuljettajan jalkatilassa, ja vuodesta 2004 se on ollut pakollinen kaikissa EU:ssa valmistetuissa autoissa. (AutoPi, 2023)

3.2.2 FlexRay

FlexRay kehitettiin aiempaa nopeamman tiedonsiirron luotettavasti mahdollistavaksi järjestelmäksi. Se suunniteltiin etenkin x-by-wire -järjestelmien, kuten steer-by-wiren eli sähköisen ohjauksen mahdollistajaksi. FlexRayn kehityksestä vastasivat alun perin BMW ja DaimlerChrysler, ja se pohjautui BMW:n aiemmin kehittämään byteflight-järjestelmään. (Schmid, n.d., s.30)

FlexRay on kustannuksiltaan muita tiedonsiirtoteknologioita kalliimpi, joten se toimii muiden, halvempien järjestelmien rinnalla. Sen etu verrattuna CAN-väylään on eri kytkentätapojen, tähti- ja hybriditopologioiden, käytön mahdollisuus. Niitä hyödyntäen useampi laite voidaan kytkeä yhteen väylässä kytkettynä olevaan, kuten Kuva 2 havainnollistetaan. Tämä lisää entisestään teknologian toimintavarmuutta. (NI, 2023)

Kuva 2, FlexRay-hybriditopologia (NI, 2023)



3.2.3 MOST

MOST (Media Oriented Systems Transport) on CAN-väylää nopeamman auton sisäisen tiedonsiirron mahdollistava järjestelmä. Siinä tieto liikkuu valokuitua pitkin 25, 50 tai

150Mbit/s nopeudella, ja siihen yhdistetyt moduulit on kytketty yleensä rengasrakenteeseen. Se kehitettiin erityisesti auton multimedialaitteita varten, joten kyberrikollisen näkökulmasta se ei ole yhtä kiinnostava kohde kuin CAN-väylä. Sen kautta voi kuitenkin saada pääsyn esimerkiksi auton mikrofoniin tai liikennetietoihin. (Smith, 2016, ss.24–25)

3.3 Automotive Ethernet

Automotive Ethernet on uusin autoteollisuuden käyttöön ottamista tiedonsiirtoväylistä. Se on tiedonsiirtonopeudeltaan edeltäjiään huomattavasti parempi, yltäen jopa 10Gbit/s nopeuksiin. On arvioitu, että se korvaa lopulta kaikki aiemmin autoissa käytössä olleet teknologiat laajan IEEE-standardisointinsa ansiosta. Standardit koskevat Ethernetin tiedonsiirtonopeuksia, kuten 100Mbit/s (IEEE 802.3bw-2015) ja 1Gbit/s (IEEE 802.3bp-2016). (Lo Bello ym., 2023)

Toistaiseksi Ethernet toimii muiden väylien rinnalla, koska monet halvoista ECUista on suunniteltu muiden väylien ehdoilla, eivätkä näin ollen tarvitse nopeampia yhteyksiä (Knight, 2020, s. xxvi).

3.4 Telematiikka

Telematiikka tarkoittaa informaatioteknologian ja automaation mahdollistamaa viestinnän ja paikkatiedon yhdistelyä. Autojen osalta se merkitsee nykyisin mm. sijainti- ja nopeustiedon keräämistä ja tallentamista. Tulevaisuudessa näitä tietoja on tarkoitus hyödyntää laajemmin autonomisen liikenteen toiminnassa, kun autot voivat kommunikoida keskenään. (Riikonen, 2022)

TCU (telematics control unit), eli telematiikan ohjausyksikkö, on auton ECUista se, joka mahdollistaa yhteyden internet- ja pilvipalveluihin, sekä Wi-Fi ja Bluetooth-yhteyksien muodostamisen. Se toimii auton sisäisten ja ulkoisten verkkojen fyysisenä välikappaleena, ja siihen yhdistyvät useimmat auton sisäisistä verkoista. TCU mahdollistaa myös useiden modernin auton ominaisuuksien, kuten langattomien järjestelmäpäivitysten ja automaattisen hätäpuhelujärjestelmän (eCall), toiminnan. (Venkat, 2020, s.3) Auton GPS-antenni on osa TCU:ta, kuten myös useat anturit, jotka mittaavat mm. kiihtyvyyttä. Lisäksi sen kautta pilveen siirtyy useiden eri ohjainlaitteiden sensoreiden dataa. (Wolbert, 2021)

4 Autojen langattomat yhteydet

Langattomien yhteyksien käyttö henkilöautoissa alkoi yleistyä 2010-luvulla Bluetoothin myötä, ja 2020-luvulla valmistetuista autoista valtaosa on varustettu sekä Bluetooth- että internetyhteyden mahdollistavalla teknologialla. Internetyhteyden muodostamiseksi autossa on joko sisäänrakennettu modeemi, tai yhteys muodostetaan käyttämällä auton matkustajan mobiililaitteen verkkoyhteyttä. (Autocrypt, 2020)

Seuraavissa luvuissa esitellään autoissa käytettävät langattomat tiedonsiirtomenetelmät ja niiden käyttökohteet.

4.1 Bluetooth

Bluetooth on verkkoprotokolla, joka kehitettiin 1990-luvun lopulla mahdollistamaan langaton viestintä lähellä toisiaan olevien laitteiden, kuten tietokoneen ja kaiuttimien, välillä. Se toimii 2,4–2,485GHz-taajuuksilla, käyttäen 79 eri kanavaa. Sen suosio kasvoi nopeasti matalien kustannusten ja helppokäyttöisyyden takia. Ensimmäiset Bluetooth-teknologiaa tukevat autot valmistettiin jo vuonna 1999, ja nykyisin se kuuluu lähes jokaisen auton vakiovarusteisiin. (Copperpod, 2022)

Autoissa Bluetoothia käytetään yleisimmin mobiililaitteen yhdistämiseksi auton järjestelmään musiikin toistoa ja puheluiden soittamista varten. Sen avulla voi myös esimerkiksi tallentaa mobiililaitteen yhteystiedot auton muistiin. (Newcomb, 2011)

4.2 Avaimeton kulku

RKE (remote keyless entry) ja PKE (passive keyless entry), ovat kaksi yleisintä auton lukitukseen käytettyä menetelmää. RKE on perinteinen malli, jossa auton avain toimii kaukosäätimenä. PKE sen sijaan mahdollistaa lukituksen avaamisen ja usein myös auton käynnistämisen ilman avaimen napin painallusta. (Shechter, 2023)

4.2.1 RKE

RKE:n käyttö alkoi yleistyä 1990-luvun lopulla, aluksi kalliimmissa autoissa. Sen käyttö kuitenkin yleistyi nopeasti, leviten kaikkiin autoihin. RKE-järjestelmä koostuu yleensä

avaimen yhteydessä olevasta radiolähettimestä, joka napin painalluksen yhteydessä lähettää signaalin autossa sijaitsevaan vastaanottimeen. Jos lähetetty signaali olisi joka kerta sama, sen nauhoittamalla voisi saada pääsyn autoon. Tämän estämiseksi käytössä on menetelmä, jossa avaimen lähettämään signaaliin lisätään salattu koodi, jota auto vertaa omaan koodiinsa. Koodi vaihtuu joka kerta, kun ovet avataan tai suljetaan, joten pelkästään koodin kaappaaminen ei riitä mahdollistamaan lukituksen avaamista myöhemmin. (Shechter, 2023)

4.2.2 PKE

PKE on RKE:n kehittyneempi versio, joka toimii muuten samalla tavalla kuin RKE, mutta lisäksi auto tunnistaa avaimen, kun se on riittävän lähellä. Tällöin lukitus voi aueta automaattisesti, tai esimerkiksi oven kahvaa koskettamalla. (Shechter, 2023)

Lähellä olevan avaimen tunnistaminen perustuu avaimessa olevan matalan taajuuden (LF) RFID-tunnisteen mahdollisuuteen kommunikoida vain parin metrin etäisyyksillä. Auto voi lähettää esimerkiksi oven kahvaa koskettaessa LF-kanavalle salatun viestin, jonka lähellä oleva avain vastaanottaa. Mikäli avain on oikea, se pystyy purkamaan salauksen ja muodostamaan halutun vastauksen, jonka se lähettää takaisin autolle, ja lukitus aukeaa. (Francillon ym., 2011)

4.3 Matkapuhelinverkko

Ensimmäiset 3G-yhteyden mahdollistavalla modeemilla varustetut autot tulivat markkinoille vuonna 2012, ja kahden vuoden kuluttua, vuonna 2014, myös LTE-yhteydellä varustetut autot saapuivat markkinoille (Compass, n.d.).

Useimmat uudet autot tukevat vähintään 4G-yhteyttä, mutta osassa on myös 5G-tuki. Ulkoiset yhteydet ovat mullistamassa autoteollisuutta, vaikuttaen vähintään turvallisuusjärjestelmien toimintaan. Samalla ne kuitenkin herättävät kuluttajissa huolta sekä kyber- että tietoturvansa osalta. (Mataciunas, 2023)

4.4 Wi-Fi

Wi-Fi on IEEE 802.11 standardiin perustuva WLAN- eli langaton lähiverkkoteknologia, joka on viime aikoina yleistynyt myös ajoneuvoissa. Niissä Wi-Fi on käytössä useimmiten kuljettajan ja matkustajien mobiililaitteiden yhdistämiseksi auton järjestelmiin, tai auton

komponenttien välisessä viestinnässä (Oka, 2021). Nykyisin auton TCU ja keskusyksikkö ovat yhä useammin yhdistetty toisiinsa Wi-Fi-yhteydellä, jonka katsotaan lisäävän potentiaalisia kyberuhkia Wi-Fi-verkkojen haavoittuvuuksien takia (Knight, 2020, s.91).

Auton Wi-Fi-reititin on toimintaperiaatteeltaan hyvin samanlainen kuin kodeissa käytetyt, joskin se käyttää usein vain 5GHz:n taajuuksia, jotka mahdollistavat nopeamman tiedonsiirron pienemmällä alueella. Joissakin autoissa käytössä on kaksi erillistä Wi-Fi-verkkoa, joista toinen on turvallisuussyistä piilotettu ja käytössä auton sisäisenä viestintäkanavana, kun taas toinen on kuljettajan ja matkustajien saatavilla. (Knight, 2018)

4.5 DSRC

DSRC (dedicated short range communications) eli lyhyen kantaman tiedonsiirto, on IEEE 802.11p-standardissa määritetty tiedonsiirtotapa, jonka toiminta perustuu WLAN-teknologiaan. Standardi koskee V2V- (vehicle-to-vehicle) ja V2I- (vehicle-to-infrastructure) yhteyksiä, eli autojen keskinäistä sekä autojen ja infrastruktuurin välistä tiedonsiirtoa, jotka ovat osa laajempaa V2X (vehicle-to-everything) -yhteyksien ryhmää. (McGrath, 2020)

Toistaiseksi DSRC-teknologiaa käytetään vain pienessä osassa markkinoiden autoista. Osuus on kuitenkin kasvamassa, ja ainakin Volkswagenin vuonna 2019 julkaisemassa Golf 8:ssa, sekä myöhemmin markkinoille tulleissa VW:n ID-sähköautoissa, DSRC on käytössä. (Gu, 2021)

DSRC:n lisäksi on toinenkin V2X-teknologia, 3GPP:n standardoima C-V2X (cellular V2X). Se toimii pitkälti samoin kuin DSRC, mutta mahdollistaa lisäksi LTE- ja 5G-yhteydet. (McGrath, 2020) Tässä työssä ei kuitenkaan käsitellä C-V2X-teknologiaa tarkemmin, sillä se ei toistaiseksi ole käytössä sarjatuotantoautoissa.

5 Kyberturvallisuus

Kyberturvallisuus on käsite, jonka määrittely yksiselitteisesti on haastavaa. EU:n verkko- ja tietoturvavirasto ENISAn määritelmässä sen sanotaan kattavan mm. kaikki kybertoimintaympäristöön negatiivisesti vaikuttavien tapahtumien estämistä, havaitsemista, analysointia ja tutkimista koskevat seikat (ENISA, 2017-b, s.6).

Kybertoimintaympäristön negatiivisiin tapahtumiin kuuluvat sekä tahattomista vahingoista johtuvat, että tahallisesti aiheutetut tapaukset (ENISA, 2017-b, s.6). Niistä jälkimmäisiin kuuluvat kyberhyökkäykset, joilla tarkoitetaan pahassa tarkoituksessa tehtyjä toimia, joilla tavoitellaan luvatonta pääsyä digitaalisiin järjestelmiin esimerkiksi niiden toimintaan vaikuttamiseksi tai tietojen varastamiseksi. Yleisiä kyberhyökkäyksiä ovat esimerkiksi väliintulohyökkäykset ja haittaohjelmat. (Cisco, n.d.-a)

Väliintulohyökkäys (man-in-the-middle-hyökkäys), tarkoittaa sellaista hyökkäystä, jossa kolmas osapuoli, eli hyökkääjä, pääsee seuraamaan kahden osapuolen välistä kommunikaatiota ja mahdollisesti myös vaikuttamaan siihen. Väliintulohyökkäykset voivat kohdistua useisiin eri kommunikaatiomuotoihin. (ENISA, n.d.) Haittaohjelma on laaja käsite, joka voi tarkoittaa monenlaisia haitallisia ohjelmia, joita kyberrikolliset käyttävät. Haittaohjelmat päätyvät järjestelmiin yleensä niistä löytyvien haavoittuvuuksien kautta, jonka jälkeen ne voivat esimerkiksi lukita järjestelmän osia, asentaa muita haitallisia ohjelmia tai kerätä tietoa järjestelmästä. (Cisco, n.d.-a)

Yleisesti voidaan sanoa, että kyberhyökkäyksen mahdollistavana tekijänä on aina jokin haavoittuvuus. Haavoittuvuuksia voi olla paitsi missä vain ohjelmistoissa, myös esimerkiksi tietoverkkojen tai laitteiden konfiguraatiossa. (Proofpoint, n.d.) Sellaisia haavoittuvuuksia, joiden olemassaolo selviää rikollisille, ennen kuin niitä on korjattu, kutsutaan nollapäivähaavoittuvuuksiksi. Niitä pystytään hyödyntämään hyökkäyksissä siihen asti, että ratkaisu korjaamiseksi ehditään toteuttaa, joten ne ovat vakava uhka. (Cisco, n.d.-a)

Hyvän kyberturvallisuuden tason saavuttaminen on vaikeutunut laitteiden määrän kasvun ja toisaalta sitä horjuttavien tahojen osaamisen kehittymisen myötä. Siksi on tärkeää huolehtia monipuolisista suojautumismenetelmistä, jotka koskevat kaikkia mahdollisesti uhattuna olevia kohteita. (Cisco, n.d.-b)

Tässä työssä luvuissa 6 ja 7 keskitytään autojen kyberturvallisuutta horjuttaviin seikkoihin, ja luvussa 8 tarkastellaan erilaisia keinoja, joilla kyberturvallisuutta on kehitetty ja kehitetään parempaan suuntaan.

6 Autoihin kohdistuvat kyberuhat ja -hyökkäykset

Autoihin kohdistuu nykyisin useita kyberuhkia, joista merkittävimpiä ovat ohjelmistojen haavoittuvuudet yhdistettynä etäyhteyden muodostamisen mahdollisuuteen sekä puutteellinen tietoturva. Myös fyysinen pääsy järjestelmiin mahdollistaa niiden toimintaan vaikuttamisen. (Gabriel-Ionel, 2023)

Hyökkäykset autojen järjestelmiin voidaan jakaa neljään ryhmään sen mukaan, millaista lähestymistapaa hyökkääjä käyttää. Langattomat yhteydet muodostavat kaksi erillistä ryhmää sen mukaan, onko kyse verkkoyhteydestä vai lyhyillä etäisyyksillä toimivasta teknologiasta, kuten Bluetoothista. Toiset kaksi ryhmää koskevat hyökkäyksiä, jotka voidaan toteuttaa auton ohjelmiston haavoittuvuuksia hyödyntäen, tai peukaloimalla auton laitteistoa fyysisesti. (Beaumont, 2023, s.7)

6.1 Tunnetut haavoittuvuudet

Autojen sisäisten tiedonsiirtoväylien kehityksen alkuaikoina autot olivat suljettuja järjestelmiä, joiden kyberturvallisuuteen ei kiinnitetty huomiota. Nopean kehityksen myötä suojaamattomat järjestelmät olivat yhä käytössä, kun ulkoiset yhteydet astuivat kuvaan. (Becsi ym., 2015, ss.3–4) Seuraavaksi käydään läpi kaksi huomiota herättänyttä tapausta, jotka langaton yhteys mahdollisti.

6.1.1 Fiat-Chrysler Uconnect

Kaksi autojen kyberturvallisuudesta huolestunutta tutkijaa, Chris Valasek ja Charlie Miller, arvelivat, että uudet teknologiat luovat turvallisuusriskejä autoilijoille. Asiaa päätettiin tutkia, ja tutkimuskohteeksi valittiin vuosimallin 2014 Jeep Cherokee sen verkkorakenteen vuoksi. Auton internet-yhteydellä varustettu radio oli yhteydessä molempiin auton CAN-väylistä, joten hypoteesina oli, että mikäli radioon saadaan muodostettua yhteys, siitä voidaan lähettää viestejä kaikkiin CAN-väylien ECUihin ja siten ottaa auton järjestelmät hallintaan. (Valasek & Miller, 2015, ss. 7–8)

Tutkijat löysivät haavoittuvuuden, joka mahdollisti pääsyn em. väyliin kaikkialta, missä auton verkko-operaattorilla oli toimintaa. Operaattori oli mahdollistanut kahden laitteen välisen kommunikoinnin verkossaan rajoituksetta. (Valasek & Miller, 2015, ss.45–46) Auton osalta haavoittuvuus koski Uconnect-tietoviihdejärjestelmän puutteellista suojausta, joka mahdollisti

etäyhteyden muodostamisen ilman minkäänlaista tunnistautumista. Kun yhteys Uconnectiin oli muodostettu, pääsi sen kautta lähettämään komentoja ECUille, ja siten vaikuttamaan mm. auton jarrujen ja ohjauksen toimintaan (CISA, 2018). Edellytyksenä tälle oli Uconnectin OMAP-prosessoriin yhteydessä olevan V850-prosessorin ohjelmiston muokkaaminen siten, että se muuntaa OMAP-prosessorilta saapuvan datan muotoon, jota CAN-väylän viesteissä käytetään. Näin täytyi toimia, koska OMAP ei voinut lähettää CAN-dataa, ja ainoastaan V850 oli yhteydessä CAN-väylään. (Valasek & Miller, 2015, ss.67–70)

Tutkijat ilmoittivat löydöksistään, ja Fiat-Chrysler reagoi nopeasti julkaisten päivityksen, jolla saapuva TCP/IP-liikene estettiin. Lisäksi laitteiden välistä kommunikointia matkapuhelinverkossa rajoitettiin operaattorin toimesta. (Valasek & Miller, 2015, s.89)

6.1.2 BMW ConnectedDrive

BMW toi 2010-luvun taitteessa kuluttajien saataville auton etähallintaa mahdollistavia ominaisuuksia (Remote Services) osana ConnectedDrive-palveluaan. Näihin palveluihin kuului muun muassa mahdollisuus avata auton lukitus mobiilisovelluksesta lähetettävällä pyynnöllä.

Palvelu herätti mielenkiintoa paitsi ominaisuuksiensa, myös sen keräämän tiedon myötä. Saksalainen autoilijoiden kerho ADAC halusi tietää tarkalleen, mitä tietoja autosta liikkuu, ja hankki asiantuntijan tutkimaan asiaa. Vaikka tutkimuksen kohteena eivät alun perin olleet järjestelmän haavoittuvuudet, tuloksista merkittävin oli kuitenkin sellainen. Takaisinmallintamalla auton telematiikkajärjestelmiä tutkija onnistui avaamaan Remote Servicellä varustettujen autojen kuljettajan oven luomalla oman verkon, jota auto piti BMW:n palvelimena. (Spaar & Scherschel, 2015)

Merkittäviä löydöksiä, jotka mahdollistivat lopputuloksen, oli useita. Samoja salausavaimia käytettiin kaikissa samalla teknologialla varustetuissa autoissa, joten hyökkäys voitiin toteuttaa myös muihin kuin alkuperäisen tutkimuksen kohteena olleeseen autoon. Liikenne auton ja palvelimen välillä käytti HTTP-protokollaa, ja siitä saatiin kerättyä miltei kaikki hyökkäystä varten tarvittava tieto. Ainoastaan kohdeauton VIN-koodi täytyi selvittää erikseen, mikä onnistui kuitenkin myös helposti. Kun kohteena olevalle autolle lähetettiin viesti väärää VIN-koodia käyttäen, se lähetti vastauksena oikean. (Spaar & Scherschel, 2015)

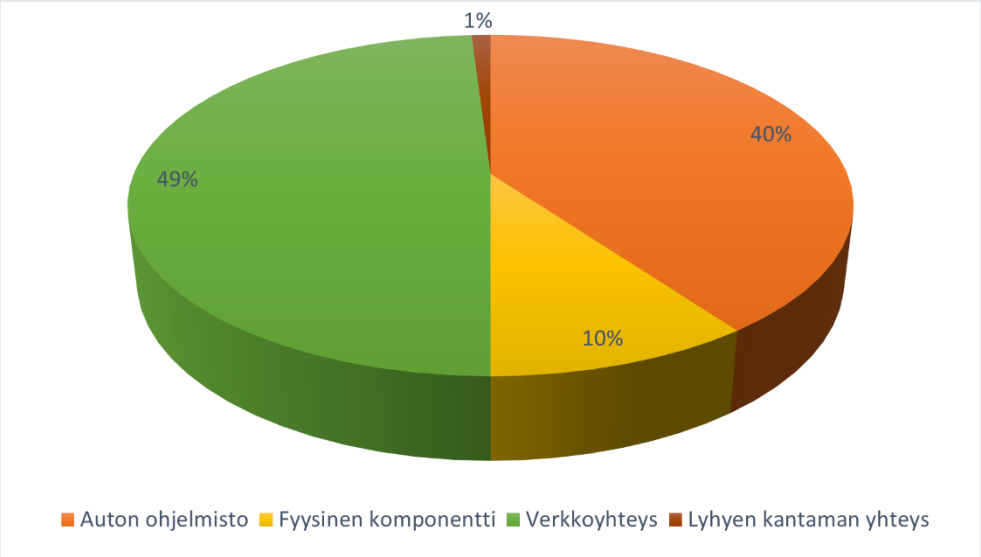
Haavoittuvuus koski yli kahta miljoonaa vuosien 2010 ja 2014 välillä valmistettua autoa, ja sen löytyminen johti toimenpiteisiin nopeasti. Autoihin asennettiin etäyhteydellä järjestelmäpäivitys, jonka myötä auton ja palvelimen välillä oli vain salattua HTTPS-liikennettä. HTTPS-protokollan käyttö poisti sekä mahdollisuuden seurata auton ja palvelimen välillä liikkuvaa tietoa, että mahdollisuuden luoda itse palvelin jäljittelemään BMW:n palvelimia. (Williams, 2015)

6.2 Uhkien kehitys

IOActive on julkaissut kolme raporttia ajoneuvojen haavoittuvuuksista. Niistä ensimmäinen koski vuosien 2012–2015, toinen 2016–2017 ja viimeisin 2018–2022 välistä ajanjaksoa. Ensimmäisen raportin julkaisuhetkellä puolet haavoittuvuuksista olivat kriittisiä tai vakavia, mutta kahdessa myöhemmässä niiden osuus laski kolmannekseen. Myös löytyneitä haavoittuvuuksia hyväksikäyttävien hyökkäysten todennäköisyyttä arvioitiin. Vuoden 2023 raportin mukaan enää alle viidesosa haavoittuvuuksista on sellaisia, joihin tullaan suurella todennäköisyydellä kohdistamaan hyökkäyksiä. (Beaumont, 2023, ss. 15–17) Kehitys on ollut lupaavaa, mutta on tärkeää tiedostaa, että se koskee vain päivitettyjä tai uusia järjestelmiä.

Haavoittuvuudet on jaettu raporteissa myös järjestelmään murtautumiseen käytettyjen menetelmien, eli hyökkäysvektoreiden, mukaan. Auton fyysisen laitteiston käyttö hyökkäysvektorina on pienentynyt merkittävästi, ja samalla auton ohjelmistojen käytön osuus on kasvanut samassa suhteessa. Verkkoyhteyksien osuus hyökkäysvektorina on pysynyt suunnilleen samana, mutta viimeisimmässä raportissa uudeksi hyökkäysvektoriksi on ilmestynyt auton lyhyen kantaman langattomia yhteyksiä, kuten Bluetoothia tai avaimetonta kulkua koskevat haavoittuvuudet. Kuva 3 havainnollistetaan vuoden 2023 raporttia mukaillen hyökkäysvektorien osuudet. (Beaumont, 2023, ss.23–24)

Kuva 3, hyökkäysvektorien jakautuminen (Beaumont, 2023, s.24)



Suurin osa autovalmistajista on kehittänyt oman mobiilisovelluksen auton hallintaan, ja kuten jo luvussa 6.1.2 kävi ilmi, myös sovellusten turvallisuuteen täytyy suhtautua vakavasti. Näin ei kuitenkaan aina ole menetelty, ja vuonna 2017 Kasperskyn seitsemään eri suuren autovalmistajan sovellukseen kohdistuneessa tutkimuksessa niistä kaikista löytyi eri asteisia puutteita, joista monet liittyivät salaamattomiin käyttäjätunnus-salasana-pareihin (Kuzin & Chebyshev, 2017). Vielä vuonna 2022 hakkerit löysivät Nissanin sovelluksesta haavoittuvuuden, jota hyödyntääkseen täytyi selvittää ainoastaan auton VIN-koodi. Sen avulla voitiin hallita kaikkia sovelluksen ominaisuuksia tai selvittää käyttäjän sovellukseen syöttämät tiedot. Sama haavoittuvuus koski myös useiden muiden autovalmistajien sovelluksia, sillä ne kaikki käyttivät saman palveluntarjoajan teknologiaa. (Toulas, 2022) Vaikuttaa siis siltä, että autoilijan kannattaa harkita kahdesti, ennen kuin ottaa auton hallintasovelluksen käyttöön mobiililaitteessaan.

6.3 Hyökkäysskenaariot

Luvuissa 6.1.1 ja 6.1.2 tutustuttiin kahteen tapaukseen, joissa tutkijat toteuttivat onnistuneesti hyökkäyksen autoa kohtaan. Molemmissa tapauksissa onnistuminen edellytti kohdeympäristön tarkkaa tutkimista, ja tiedonsiirtoon käytettyjen menetelmien toiminnan selvittämistä. Seuraavissa luvuissa käydään läpi yleisellä tasolla mahdollisia hyökkäysten toteutustapoja ja niiden seurauksia.

6.3.1 Etäyhteydellä toteutettavat hyökkäykset

Etänä tapahtuvassa hyökkäyksessä hyökkääjä pyrkii muodostamaan yhteyden auton tietoviihdejärjestelmään tai telematiikan ohjausyksikköön, ja sitä kautta hallitsemaan auton väyläjärjestelmiin kytkettyjä ohjainlaitteita (ENISA, 2017-a, s.33).

Tämän kaltaisen hyökkäyksen toteuttaminen on monivaiheinen prosessi, ja kaikki tunnetut tapaukset on toteutettu tutkimusolosuhteissa. Niissä hyökkäyksen alkuvaiheessa hyökkääjä on muodostanut jotakin man-in-the-middle-hyökkäyksen muotoa käyttäen yhteyden autoon, joko mobiiliverkon kautta, tai hankkimalla pääsyn auton Wi-Fi-verkkoon. Kun yhteys on muodostettu, hyökkääjällä on pääsy auton tietoviihdejärjestelmään. Nykyautoissa se on yhteydessä yhdyskäytävään, johon myös auton sisäiset tiedonsiirtoväylät ovat yhteydessä. (Huq ym., n.d., s.12)

Käytännössä hyökkääjän täytyy yhteyden muodostamisen jälkeen onnistua jotakin ohjelmiston haavoittuvuutta hyödyntäen avaamaan komentorivi-istunto. Jos käyttöoikeudet tässä vaiheessa eivät riitä, hyökkääjän täytyy vielä jonkin toisen haavoittuvuuden avulla saada pääkäyttäjän oikeudet, jotta tämä pääsee toimimaan vapaasti kohdeympäristössä. Seuraavassa, ja hyökkäyksen kannalta kriittisimmässä vaiheessa hyökkääjän täytyy korvata yhdyskäytävän ECUn ohjelmisto muokatulla versiolla, joka mahdollistaa CAN-viestien lähettämisen sen kautta. Jos tässä vaiheessa jokin epäonnistuu, voi ECUn toiminta lakata täysin, johtaen hyökkäyksen keskeytymiseen. Joissakin tapauksissa tätä vaihetta ei kuitenkaan tarvita, jolloin tavoitteen saavuttaminen on yksinkertaisempaa. (Huq ym., n.d., s.12) Yleisesti ottaen voidaan kuitenkin todeta, että tällaisen hyökkäyksen uhriksi joutumisen riski on hyvin pieni sen monimutkaisuuden vuoksi (ENISA, 2017-a, ss.34–35).

6.3.2 Lyhyen kantaman yhteyksiin kohdistuvat hyökkäykset

Tunnetuimpia auton lyhyen kantaman yhteyksiä hyödyntäviä hyökkäyksiä ovat erilaiset avaimettoman kulun haavoittuvuuksiin kohdistuvat hyökkäykset, joiden avulla hyökkääjä saa pääsyn autoon tai voi varastaa sen.

Roll jam -hyökkäyksessä, joka kohdistuu RKE-järjestelmää käyttävään autoon, hyökkääjän täytyy nauhoittaa avaimesta lähtevä signaali, kun auton kuljettaja on avaamassa lukitusta, ja samalla häiritä signaalia siten, että auto ei tunnista sitä oikeaksi. Kun kuljettaja yrittää avata ovet uudestaan, hyökkääjä nauhoittaa myös tämän signaalin. Seuraavaksi hyökkääjä

lopettaa häirinnän ja toistaa ensin nauhoittamansa signaalin, jolloin lukitus aukeaa. Jälkimmäinen signaali ei siis tässä vaiheessa saavuta autoa, mutta on hyökkääjällä tallennettuna. Kun hyökkääjä myöhemmin toistaa tämän signaalin, auton lukitus aukeaa. (Shechter, 2023)

Toisin kuin roll jam -hyökkäys, PKE-järjestelmään kohdistuva välityshyökkäys mahdollistaa myös auton käynnistämisen. Sen toteuttamiseksi hyökkääjiä tarvitaan kaksi, joista toinen on kohdeauton luona ja toinen avaimen lähellä. Auton luona oleva hyökkääjä yrittää avata oven, jolloin auto lähettää signaalin avaimelle. Kuten luvussa 4.2.2 kerrottiin, avaimen täytyy olla parin metrin säteellä autosta, jotta signaali kulkisi sille asti. Tämän rajoituksen kiertääkseen hyökkääjä välittää signaalin avaimen lähellä olevalle kumppanilleen, joka lähettää sen edelleen avaimelle. Kun sama toistetaan toiseen suuntaan, lukitus aukeaa, ja samalla menetelmällä auto voidaan myös käynnistää. (Shechter, 2023)

6.3.3 Fyysistä pääsyä edellyttävät hyökkäykset

Hyökkäykset, joissa hyökkääjällä täytyy olla fyysinen pääsy järjestelmään, kohdistuvat useimmiten auton OBD2-porttiin, joka tarjoaa suoran pääsyn CAN-väylään. Myös USB-portti voi olla tällaisen hyökkäyksen kohteena, koska se on yhteydessä auton tietoviihdejärjestelmään, joka taas on usein yhteydessä CAN-väylään. Molemmissa tapauksissa tavoitteena on päästä vaikuttamaan väylään kytkettyjen ohjainlaitteiden toimintaan. (Checkoway ym., 2011)

Hyökkäyksen toteuttaminen voi edellyttää esimerkiksi luvussa 6.3.2 mainittujen tekniikoiden käyttöä. Toisaalta myös käyttäjää manipuloimalla tämän voi saada liittämään viruksen sisältävän USB-tikun järjestelmäänsä (Checkoway ym., 2011).

Fyysistä pääsyä vaativia uhkia liittyy myös yleistymässä olevaan sähköautoiluun. Vuonna 2021 16:ta eri sähköauton latausasemaa tutkinut ryhmä löysi tutkimuksessaan niistä jokaisesta haavoittuvuuksia (Nasr, ym., 2021, s.15).

Upstreamin julkaisemassa raportissa arvioidaan, että 4 %:ssa kaikista autoiluun liittyvistä tapauksista hyökkäysvektorina toimii sähköautojen latausinfrastruktuuri. Haavoittuvaista latausasemaa voidaan hyödyntää pääsynä latausasemien hallintaverkkoon, ja sitä kautta muiden latausasemien toimintaan voidaan päästä vaikuttamaan. Tätä kautta voi mahdollistua

myös pääsy hyökkäyksen kohteeksi päätyneellä asemalla ladattavan auton sisäisiin verkkoihin. (Upstream, 2023, ss.18–22)

7 Valmistajien tiedonkeruu

Autoteollisuuden digitalisaation edetessä autoihin alettiin asentaa paitsi langattomat yhteydet mahdollistavia, myös telemetristä dataa kerääviä yksiköitä, joista kerrottiin luvussa 3.4. Kerätty data voidaan jakaa kahteen kategoriaan sen mukaan, voidaanko siitä tunnistaa henkilö, jonka data on kyseessä. (AutoPi, 2022)

Data, jota ei voi yhdistää auton kuljettajaan, käsittää esimerkiksi ajoneuvon kunnosta ja huolloista kertovia tietoja, sekä ympäristötekijöihin, kuten säätilaan ja tien kuntoon liittyvää dataa. Henkilökohtainen, suoraan kuljettajaan yhdistettävissä oleva data voi käsittää mm. ajotapaan ja kuljettuun reittiin liittyviä asioita, ja lisäksi autoon yhdistetyn mobiililaitteen auton kanssa vaihtamia tietoja. (AutoPi, 2022)

Mozilla Foundation julkaisi vuonna 2023 tulokset tutkimuksestaan, jossa 25:n suuren autoteollisuuden yrityksen tiedonkeruuta tarkasteltiin kuluttajan tietoturvan näkökulmasta. Tulokset paljastivat, että lähes jokainen valmistaja kerää kaiken saatavilla olevan tiedon, ja suurin osa myös jakaa tai myy tätä tietoa eteenpäin. (Caltrider ym., 2023)

Mozillan tutkimuksessa parhaiten menestyivät Renault ja Renaultin omistama Dacia, sillä ne olivat ainoat merkit, jotka tarjosivat kaikille kuljettajille oikeuden heitä koskevan datan poistoon. BMW, Fiat-Chrysler ja Subaru arvioitiin seuraavaksi eniten kuljettajan tietosuojasta välittäväksi, ja suurin osa muista merkeistä (mm. Audi, Nissan ja Mercedes-Benz) olivat lähellä samaa tasoa niiden kanssa. Ainoastaan Tesla oli tätä huonompi, ja hävisi koko vertailun autopilottinsa epävarman toiminnan vuoksi. (Caltrider ym., 2023)

Vaikka tutkimuksen löydökset vaikuttavat huolestuttavilta, on huomioitava, että se tehtiin USA:ssa. EU:n alueella GDPR (General Data Protection Regulation) eli EU:n yleinen tietosuoja-asetus määrittää tarkasti tiedon keräämiseen ja käsittelyyn sekä kuluttajan oikeuksiin liittyviä seikkoja. Seuraavissa luvuissa luodaan katsaus kolmen Suomessa viime vuosina paljon ensirekisteröidyn automerkin valmistajien tietosuojaselosteisiin, ja kyberturvallisuusuhkiin, jotka koskevat kerättyä tietoa.

7.1 Tilanne Suomessa

Suomessa ensirekisteröitiin vuosina 2022 ja 2023 yhteensä noin 170 000 henkilöautoa, joista lähes neljänneksen muodostivat Skodan, Volvon ja Teslan yhteenlaskettu osuus. Näistä

merkeistä jokaisen rekisteröinnit myös kasvoivat vuodesta 2022 vuoteen 2023. (Autoalan Tiedotuskeskus, 2024) Tässä luvussa tarkastellaan näiden merkkien tietosuojaselosteita kiinnittäen erityistä huomiota kuluttajan mahdollisuuksiin vaikuttaa kerättyyn tietoon.

Skodan tietosuojalausunnossa painotetaan henkilötietojen käsittelyn noudattavan lainsäädäntöä, ja yritys kertoo suhtautuvansa vakavasti tietojen suojaamiseen. Tietojen käsittelyn yleisiä syitä ovat mm. huoltopalveluiden ja mobiilisovelluksen käyttö, joiden yhteydessä tietojen käsittelyn oikeudellisena perustana on sopimuksen solmiminen. Markkinointitarkoituksessa tapahtuvaan tietojen käsittelyyn kuluttaja pystyy vaikuttamaan, ja sitä ei tapahdu ilman erillistä suostumusta. (Skoda, n.d.-a)

Lausunnossa henkilötiedot on jaettu useaan eri kategoriaan, joihin kuuluvat esimerkiksi tunnistavat tiedot, yhteystiedot, riskiprofiilit, kuvailevat tiedot ja paikannustiedot (Skoda, n.d.-a). Siinä ei kuitenkaan eritellä tarkemmin, missä yhteyksissä ja miten eri kategorioiden tietoja kerätään.

Skodan digitaalisten tuotteiden, kuten mobiilisovelluksen ja ajoneuvon tietoviihdejärjestelmän, tietosuojailmoituksessa kerrotaan tarkemmin niiden yhteydessä käytetyistä henkilötiedoista. Kaikkia digitaalisia tuotteita varten kerätään tunniste-, yhteys-, ja sijaintitietoja, tietoa kommunikointitavoista, kuvailevia tietoja, verkkotunnisteet, sekä tuotteen eli esimerkiksi ajoneuvon teknisiä tietoja. (Skoda, n.d.-b) Nämä tiedot voivat sisältää mm. nimen, henkilötunnuksen ja osoitteen, sekä tietoa vapaa-ajanvietosta ja ajotyylistä (Skoda, n.d.-a). Näiden tietojen keräämiseltä ja käsittelyltä välttymiseksi on siis pidättäydyttävä käyttämästä mitään Skodan digitaalisia palveluita, joihin ainakin joiltain osin myös auton tietoviihdejärjestelmä kuuluu.

Volvon verkkosivuilta on saatavilla kolme erillistä kuluttajan kannalta merkityksellistä tietosuojailmoitusta, joista ensimmäinen on Volvo Carsin yleinen tietosuojailmoitus, toinen koskee autoja ja kolmas sovellusta. Yleisessä tietosuojailmoituksessa kerrotaan lähinnä henkilötietojen käytöstä muissa kuin autoiluun liittyvissä yhteyksissä. Siitä löytyy myös sanasto, jossa kerrotaan tarkemmin eri yläkäsitteiden sisällään pitämistä tiedoista. (Volvo, 2024-b) Volvon mobiilisovelluksessa tietojen käsittely perustuu tietosuojailmoituksen mukaan sopimukseen, jonka lisäksi joidenkin tietojen käsittelystä, esimerkiksi yhteystietoja kuljettajan mobiililaitteesta autoon siirrettäessä, kysytään käyttäjältä erikseen. Sovelluksen käyttö tarkoittaa kuitenkin vähintään laite- ja käyttötietojen sekä auton yleisien tietojen keräämistä. (Volvo, 2024-a)

Volvon autojen tietosuojailmoituksessa eri palvelut ja järjestelmät, sekä tiedot, joita niiden yhteydessä käsitellään, on eritelty omiin kappaleisiinsa. Tiedon käsittelyn peruste mainitaan jokaisessa kohdassa, ja osassa niistä myös tuodaan ilmi mahdollisuus lopettaa palvelun käyttö ja samalla siihen liittyvä tiedon käsittely. Suurimmassa osassa tapauksista käsiteltävät tiedot koskevat lähinnä auton teknisiä tietoja, mutta joissakin yhteyksissä, kuten auton joutuessa onnettomuuteen, myös esimerkiksi henkilö- ja kameratietoja käsitellään. Ilmoituksessa mainitaan erikseen, että viranomaistiedustelujen yhteydessä henkilötietoja ei luovuteta, ellei laki sitä erikseen vaadi. (Volvo, 2023)

Teslan tietosuojailmoituksen mukaan ajoneuvo luo siihen liittyviä diagnostiikkatietoja, sekä tietoviihde- ja Autopilot-järjestelmiin liittyviä tietoja. Näistä Autopilot-järjestelmän tietojen luvataan pysyvän oletusarvoisesti vain auton sisällä. Ajoneuvosta kerättyihin tietoihin kuuluvat paitsi telemetriset ja diagnostiikkatiedot, myös mobiilisovelluksen käyttöä koskevat tiedot. Kerätyistä tiedoista kerrotaan melko suppeasti, ja monessa kohdassa mainitaan, että muutakin kuin kohdassa mainittua tietoa voidaan kerätä, sitä sen tarkemmin yksilöimättä. (Tesla, 2024)

Tesla tarjoaa mahdollisuuden lopettaa tietojen kerääminen ajoneuvosta, mutta sen mahdollisiksi seurauksiksi mainitaan toimintojen rajoittaminen tai jopa auton toiminnan lakkaaminen. (Tesla, 2024)

Jokaisessa tietosuojailmoituksessa on kerrottu kuluttajan oikeuksista pyytää datan poistoa, ja tilanteista, joissa se on mahdollista. Se vaikuttaa olevan ainoa merkittävä ero Mozillan tutkimuksessa esille nostettuihin huolenaiheisiin.

7.2 Tiedonkeruun riskit

Auton järjestelmien keräämä tai kuljettajan toimesta luotu data voi päätyä kolmansille osapuolille paitsi edellä kerrotun mukaisesti, myös kyberrikollisten toimien kautta.

Pilveen siirtyvä data voi päätyä rikollisten haltuun, jos he onnistuvat pääsemään samaan verkkoon, johon auto on yhdistettynä. Kyse voi olla sekä Wi-Fi-, että mobiiliverkosta, jonka liikennettä nauhoittamalla hyökkääjä voi päästä tarkastelemaan sitä. (Bakhshiyeva & Berefelt, 2022, s.21) Lähtökohtaisesti auton ja palvelinten välinen data siirretään salatussa muodossa, jolloin sen päätymisen rikollisille ei pitäisi johtaa ikäviin seurauksiin. Todennäköisempää onkin, että rikolliset pyrkivät pääsemään käsiksi niihin palvelimiin, joilla

autoista kerättyä dataa säilytetään. (Stevens, 2023) Auton järjestelmissä salaamattomassa muodossa tallennettuna oleva data taas voi päätyä rikollisille esimerkiksi jonkin luvussa 6.3 kuvatun hyökkäyksen seurauksena.

8 Turvallisuusprotokollat ja -ratkaisut

Kyberturvallisuus on muodostunut kasvavaksi huolenaiheeksi autoteollisuudessa, ja sen parantamiseksi on alettu käyttämään erilaisia menetelmiä, kuten palomuureja ja salausta. Päivitysten saatavuutta on parannettu, ja autojen järjestelmiä tarkkaillaan reaaliajassa uhkien havaitsemiseksi. (Meah, 2023)

Alun perin kyberturvallisuuden kehittämistä ohjasivat vain suositukset, mutta niiden rinnalle on luotu myös sääntelyä, joka velvoittaa valmistajia toimimaan tietyllä tavalla (Ungurean, n.d.). Seuraavissa luvuissa käydään läpi autoalalla käytössä olevaa sääntelyä ja menetelmiä, joiden tavoitteena on kyberturvallisuuden parantaminen.

8.1 Päivitysmekanismit ja haavoittuvuuksien hallinta

Modernien autojen ohjelmistot ohjaavat lähes kaikkia auton komponentteja, ja toiminnan varmistamiseksi ohjelmistoja täytyy myös päivittää. Autojen langattomien yhteyksien kehitys mahdollistaa ohjelmistojen päivittämisen etäyhteydellä, ilman fyysistä huoltokäyntiä. Tällaisella ominaisuudella varustetussa autossa päivityksestä tulee useimmiten ilmoitus auton näytölle, ja asentamisen voi suorittaa auton ollessa pysäköitynä. Perinteisiin päivitysmenetelmiin verrattuna etäpäivityksien asentamiselle arvellaan olevan matalampi kynnys, sekä helppouden, että ajan ja rahan säästymisen vuoksi. Tämä vaikuttaa positiivisesti myös kyberturvallisuuteen, kun järjestelmien haavoittuvuudet korjaavat päivitykset saadaan toimitettua kuluttajille aiempaa tehokkaammin. (Cinch, n.d.)

Myös etäpäivityksiin liittyy kuitenkin omat riskinsä, jos järjestelmiä ja päivitystiedostoja ei suojata asianmukaisesti. Siksi valmistajien suositellaan huolehtivan päivitysten ja niitä toimittavien palvelinten, sekä lähetysmekanismin ja itse päivitysprosessin turvallisuudesta. (NHTSA, 2022, s.18) On myös hyvä huomioida, että pian valmistajat ovat velvoitettuja toimimaan em. tavalla päivitystensä kanssa. Tästä kerrotaan tarkemmin luvussa 8.2.3.

8.2 Standardit ja sääntely

Autoilun turvallisuus on ollut huolenaihe jo kauan, ja sen parantamiseksi on kehitetty paljon erilaisia varusteita ja järjestelmiä. Näiden järjestelmien käyttöä on ohjailtu standardeilla ja lainsäädännöllä. Esimerkiksi Euroopan Komission asetus 661/2009 toi pakollisiksi

elektronisen ajonvakautusjärjestelmän, automaattisen hätäjarrujärjestelmän sekä kaistanvaihdon varoitusjärjestelmän (European Commission, n.d.).

Vastaava menettely on viime vuosina alkanut yleistymään myös autojen kyberturvallisuuteen liittyvien järjestelmien osalta. Seuraavissa luvuissa käydään lyhyesti läpi keskeisimmät autojen kyberturvallisuuteen liittyvät standardit ja asetukset.

8.2.1 SAE J3061

SAE (Society of Automotive Engineers) J3061-standardi, joka tunnetaan myös nimellä Cybersecurity Guidebook for Cyber-Physical Vehicle Systems, julkaistiin alun perin vuonna 2016 aiempien autoteollisuuden käytäntöjen ja säännösten pohjalta. Nykyinen, päivitetty versio on vuodelta 2021. (SAE International, 2021)

Standardin suositellut käytännöt vakiinnuttavat korkean tason ohjeistusta kyberfyysisen, eli fyysistä ja digitaalista järjestelmää yhdistelevän, ajoneuvojärjestelmän kyberturvallisuudesta. Ne sisältävät mm. määritelmän kyberfyysisen järjestelmän elinkaaren prosesseista, joita yritysten tulisi hyödyntää tuotteiden suunnittelusta alkaen niiden käytöstä poistoon asti, ja tietoa käytössä olevista työkaluista ja menetelmistä kyberfyysisten järjestelmien suunnittelu- ja vahvistusvaiheissa. (SAE International, 2021)

8.2.2 ISO/SAE 21434

ISO/SAE 21434 -standardi on ISO:n ja SAE:n, sekä useiden autoteollisuuden yritysten ja kyberturvallisuusasiantuntijoiden yhteistyön tulos. Tarve yhdenmukaistaa termien käyttöä yritysten välillä ja määrittää riittävän kyberturvallisuuden käsite olivat suurimmat syyt standardin luomiseen. Tavoitteena sillä on parantaa erityisesti autoilijan turvallisuutta, ja siksi riskien ja niiden torjumiseen tarvittavien toimien määrittely on tehty sen mukaan, millainen vaikutus niillä on autoilijaan. (Goldstein, 2020)

Standardi julkaistiin vuonna 2021, ja se korvasi aiemmin käytetyn SAE:n J3061-standardin. Standardia ei kuitenkaan pidetä täydellisenä, koska se määrittää ainoastaan tavoitellut tulokset. Esimerkiksi ISO 26262-standardissa, joka määrittelee autojen toiminnallista turvallisuutta, myös menetelmät tulosten saavuttamiseksi on määritelty. (Pitchford, 2022)

ISO/SAE 21434:ssä kuvataan TARA (Threat Agent Risk Assessment) -prosessi. Sen tarkoitus on auttaa tunnistamaan, arvioimaan, priorisoimaan ja kontrolloimaan kyberturvallisuusriskejä. Riskin vakavuuden taso määritellään sen tyypin, vaikutuksen, hyökkäysvektorin ja hyökkäyksen tyypin ja -vektorin yhteensopivuuden pohjalta. Vaikutukset on jaettu niiden vakavuuden mukaan neljään ryhmään, ja lisäksi jako on tehty sen mukaan, onko vahinko fyysistä, rahallista, toiminnallista vai yksityisyyteen liittyvää. (Pitchford, 2022)

8.2.3 UNECE WP.29 R155 & R156

UNECE:n (United Nations Economic Commission for Europe), eli Yhdistyneiden Kansakuntien Euroopan talouskomission, työryhmä WP.29 (World Forum for Harmonization of Vehicle Regulations) julkaisi vuonna 2021 asetukset R155 ja R156. Ne velvoittavat UNECE:n jäsenmaiden autoteollisuutta, ja vuoden 2022 heinäkuusta lähtien niiden noudattaminen on ollut edellytyksenä uusien automallien tyyppihyväksynnälle. Vuoden 2024 heinäkuusta alkaen asetusten noudattamista aletaan vaatimaan kaikkien valmistettavien autojen osalta, joitakin poikkeuksia lukuun ottamatta. (Strzalkowski, 2023)

Asetuksessa 155 määritetään kyberturvallisuuden hallintajärjestelmän (CSMS, Cyber Security Management System) vaatimuksenmukaisuustodistuksen hakuprosessin kulku ja vaatimukset todistuksen saamiseksi. Tällaisia vaatimuksia ovat mm. hallintajärjestelmän käyttö kehitys- ja tuotantovaiheissa sekä tuotannon jälkeen ja riskien tunnistamiseen käytettyjen menetelmien asianmukaisuus. (UNECE, 2021a)

Asetus 156 asettaa yhdenmukaiset vaatimukset autojen ohjelmistopäivityksille ja ohjelmistopäivitysten hallintajärjestelmälle (SUMS, Software Update Management System). Sen turvallisuuteen liittyvissä vaatimuksissa on mainittu mm. päivitystiedostojen manipulaation estäminen, käytettyjen menetelmien asianmukainen suojaaminen, ja aiemman järjestelmäversion palauttamisen mahdollisuus, mikäli jokin päivityksessä epäonnistuu. (UNECE, 2021b)

8.3 Salausmenetelmät

NHTSA:n (National Highway Traffic Safety Administration) autojen kyberturvallisuuden parhaat käytännöt -julkaisussa suositellaan salauksen käyttöä osana autojen kyberturvallisuuden kehittämistä. Huomiota tulisi kiinnittää erityisesti menetelmien ajantasaisuuteen, sekä niiden toteutuksen turvallisuuteen. Suosituksissa mainitaan salattujen

käyttäjätunnusten, PKI:n (Public Key Infrastructure) ja salausavainten käyttö, ja painotetaan, että yhden auton järjestelmästä löytyvät tunnukset eivät saa mahdollistaa pääsyä jonkin toisen auton järjestelmään. (NHTSA, 2022, s.14)

PKI, eli julkisen avaimen infrastruktuuri, on käyttäjien ja laitteiden aitouden varmistamiseksi käytetty teknologia. Se perustuu luotettujen tahojen, varmentajien, myöntämien varmenteiden käyttöön. Varmenne osoittaa, että tietty avain kuuluu esimerkiksi tietylle käyttäjälle tai laitteelle, ja sitä voidaan käyttää kyseisen käyttäjän tai laitteen tunnistamiseen. PKI käyttää epäsymmetristä salausta, eli siinä jokaisella osapuolella on kaksi avainta, yksityinen ja julkinen. Yksityinen avain on vain tiedon lähettäjän tiedossa, ja sitä käytetään tiedon digitaaliseen allekirjoitukseen. Vastaanottaja voi lähettäjän julkisella avaimella tarkistaa, onko lähettäjä se, joka väittää olevansa. (SSH, n.d.)

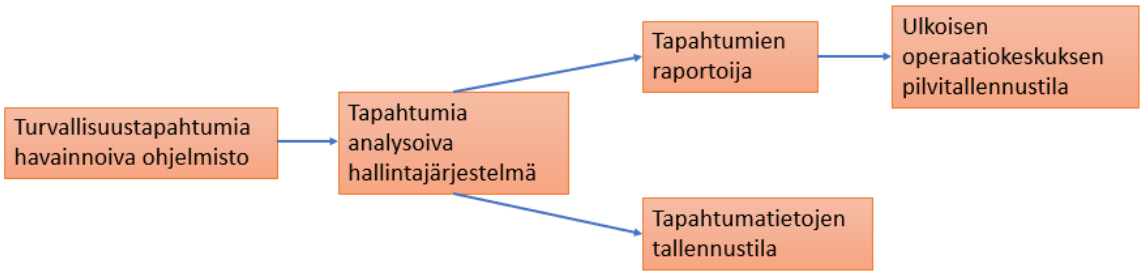
Yleisintä PKI:n käyttö on SSL (Secure Sockets Layer) -varmenteissa. SSL, samoin kuin sen uudempi versio TLS (Transport Layer Security), ovat verkon turvallisuusprotokollia, joita käytetään verkkosivujen varmentamiseksi. Kun SSL tai TLS on käytössä, verkkosivun ja laitteen välinen liikenne on salattu, eikä kolmas osapuoli voi vaikuttaa siirtyvään dataan. (SSH, n.d.)

8.4 IDS

Tunkeutumisen havaitsemisjärjestelmät (IDS, Intrusion Detection System) on kehitetty tarkkailemaan verkkoliikennettä, ja varoittamaan epäilyttävästä toiminnasta. Järjestelmiä on käytössä nykyisin ainakin osalla autovalmistajista, kuten Audilla, Mercedes Benzillä ja BMW:llä. (Hurtado, 2023)

Autoteollisuudessa tunkeutumisen havaitsemisjärjestelmä koostuu viidestä osasta, jotka on kuvattu Kuva 4. Osista neljä on autossa, jossa ne havainnoivat, analysoivat, tallentavat ja välittävät eteenpäin tietoa epäilyttävistä tapahtumista. Viides osa, ulkoinen operaatiokeskus, saa tiedon tapahtumasta, ja siellä työntekijät ryhtyvät asianmukaisiin toimiin löydösten pohjalta estääkseen vastaavat tapahtumat tulevaisuudessa. (Vector, n.d.)

Kuva 4, tunkeutumisen havaitsemisjärjestelmän toiminta Vectorin kuvaa mukaillen (Vector, n.d.)



8.5 Avainten suojamekanismit

Luvussa 6.3.2 kerrottiin välityshyökkäyksestä, joka mahdollistaa autoon murtautumisen ja sen varastamisen auton ja avaimen välisen kommunikoinnin haavoittuvaisuuden vuoksi.

Hyökkäyksien ehkäisemiseksi on kehitetty erilaisia menetelmiä, joista yksi on aikakatkaisun lisääminen osaksi järjestelmää. Sitä käyttävä järjestelmä kytkeytyy pois päältä, kun auton ja avaimen kommunikaatiolle asetettu aika ylittyy. Tällaisen suojauksen toteuttaminen onnistuu kohtuullisen helposti, sillä signaali kulkee aina samalla nopeudella. Tämän pohjalta on helppo laskea esimerkiksi muutaman metrin päässä autosta olevalle avaimelle ja siltä takaisin välittyvälle signaalille tarvittu aika, ja käyttää sitä raja-arvona (Shechter, 2023).

Toinen tehokas keino on liiketunnistimen lisääminen avaimeen. Tässäkin tapauksessa aikakatkaisu kytkee järjestelmän pois käytöstä, joskin avaimen paikallaanoloajan perusteella. Esimerkiksi minuutin liikkumattomuuden jälkeen avain deaktivoituu, eikä vastaa autolta tuleviin signaaleihin, ennen kuin sitä liikutetaan uudestaan (Shechter, 2023).

9 Riskien kartoittaminen ja CAN-viestinnän takaisinmallinnus

Työn käytännön osassa kartoitettiin vuosimallin 2023 Skoda Karoqin langattomia yhteyksiä käyttävien järjestelmien riskejä teoriaosassa esitetyn tiedon pohjalta. Jatkona tälle selvitettiin myös, miten auton sisäisten tiedonsiirtoväylien viestinnän takaisinmallintaminen ja niissä liikkuvan datan manipulointi onnistuu käytännössä, koska se on joidenkin vakavampia seurauksia aiheuttavien hyökkäysten tavoitteena. Kohteeksi valittiin CAN-väylä, koska auton toiminnan kannalta olennaisimmat ohjainlaitteet on yleensä kytketty siihen.

Seuraavissa luvuissa käydään läpi riskikartoituksen perustana käytetty prosessi, sekä kuvataan lyhyesti työkalut ja ohjelmat, joita CAN-viestinnän takaisinmallinnuksessa käytettiin. Lopuksi esitellään riskikartoituksen tuloksia, sekä takaisinmallinnusprosessi.

9.1 Riskienhallintaprosessi

Riskienhallintaprosessi alkaa toimintaympäristön määrittelyllä. Siinä päätetään, mitä riskien arviointiin sisällytetään ja mitä jätetään sen ulkopuolelle, ja määritetään todennäköisyyttä ja riskitasoa arvioitaessa käytettävät kriteerit (Rousku, 2017, s.19).

Riskien arviointiprosessi on osa riskienhallintaprosessia. Se koostuu riskien tunnistamisesta, analysoinnista ja merkityksen arvioinnista. Riskien tunnistamisen tavoitteena on kaikkien merkityksellisten riskien ja niihin liittyvien tekijöiden havainnointi. Myös erilaisesta riippuvuuksista johtuvat riskit tulee huomioida. Edellytyksenä onnistuneelle riskien tunnistamiselle on siitä huolehtivan henkilön riittävä asiantuntemus. (Rousku, 2017, ss.21–22)

Riskianalyysissä luodaan perusta riskien käsittelyyn liittyville päätöksille. Analyysi perustuu sitä tekevän henkilön omiin arvioihin, jotka voivat olla joko sanallisia tai numeerisesti esitettyjä. Riskit, jotka liittyvät turvallisuuteen, voidaan yleensä arvioida numeerisesti niiden toteutumisen todennäköisyyden ja vaikutusten osalta käyttäen neliportaista asteikkoa. Asteikolla 1 on epätodennäköinen riski tai riski, jonka toteutumisen seuraukset ovat vähäisiä, ja 4 lähes varma tai toteutuessaan kriittisiä seurauksia aiheuttava riski. Riskien merkitystä arvioidessa lasketaan riskin suuruus kertomalla riskin toteutumisen todennäköisyyden ja sen vaikutusten arvot keskenään. Riskin suuruuden mukaan määritetään, vaatiiko riski toimenpiteitä, ja millä aikataululla siitä pitää huolehtia. (Rousku, 2017, ss.22–25)

Riskien käsittelyvaiheessa määritetään riskikohtaiset toimenpiteet ja niiden tekijät. Toimenpiteisiin voi kuulua mm. riskin torjuminen pidättäytymällä riskejä aiheuttavasta toiminnasta, sen toteutumisen todennäköisyyteen tai seurauksiin vaikuttaminen tai myös tilanteen säilyttäminen ennallaan. (Rousku, 2017, s.26)

9.2 Käytetyt työkalut ja ohjelmat

Työn vaihe, jossa tutkittiin CAN-väylän liikennettä, suoritettiin Kali Linux 2023.4 -virtuaalikonetta käyttäen. Kali Linux on Debian-pohjainen Linux-ympäristö, johon on esiasennettu mm. penetraatiotestaukseen ja takaisinmallinnukseen käytettäviä ohjelmia (Kali Org, n.d.). Kalin esiasennettujen ohjelmien lisäksi siihen asennettiin can-utils-työkalut ja ICSim-ohjelmisto.

ICSim on virtuaalisen auton mittariston ja siihen CAN-väylällä yhdistyvän ohjainpaneelin luomiseen käytettävä ohjelmisto, jonka avulla voi tutustua CAN-viestien takaisinmallinnukseen. Sen lähdekoodi ja ohjeita sen käyttöönottoon on saatavilla osoitteesta https://github.com/zombieCraig/ICSim (Smith, 2016, s.81).

9.3 Auton järjestelmien riskikartoitus

Riskien kartoittaminen tehtiin käyttäen ohjenuorana luvussa 9.1 kuvattua prosessia. Kartoituksen kohteena oli vuosimallin 2023 Skoda Karoq -henkilöauton telematiikka-, tietoviihde- ja avaimettoman kulun järjestelmät. Tarkemmin sanottuna kyse oli ohjainlaitteiden J949 (Emergency call module control unit and communication unit), J794 (Control unit 1 for infotainment electronics) sekä J965 (Interface for entry and start system) ja J519 (Onboard supply control unit) toimintaan liittyvien riskien tarkastelusta.

Riskikartoitus rajattiin koskemaan vain kyberrikollisuutta koskevia riskejä, joten esimerkiksi laiterikkoihin tai sääolosuhteisiin liittyvät riskit jätettiin kartoituksen ulkopuolelle. Riskien vaikutusta arvioitiin asteikolla 1–4 sen mukaan, miten vakavia seuraukset pahimmillaan voisivat olla. Lievänä vaikutuksena pidettiin esimerkiksi tilannetta, jossa hyökkääjä saa haltuunsa pelkästään dataa, ja vakavana sellaista, jossa hyökkääjän toimet voivat johtaa jopa hengenvaarallisiin tilanteisiin auton käyttäjälle. Todennäköisyyden arvioinnissa tarkasteltiin riskin toteutumiseen vaadittavia ehtoja, joiden määrän kasvaessa arvioitiin todennäköisyyden pienenevän. Riskit listattiin Excel-taulukkoon, joka on nähtävissä liitteessä 2.

Karoqin tietoviihde- ja telematiikkajärjestelmät pohjautuvat Volkswagen Groupin kolmannen sukupolven MIB-järjestelmään (Skoda Storyboard, 2020). Siinä J949 vastaa LTE-yhteyksistä, ja J794 Wi-Fi ja Bluetooth-yhteydestä. Auton matkustamon USB-portit ovat yhteydessä J794:n. Sekä J949 että J794 yhdistyvät CAN-väylän kautta auton yhdyskäytävään, jonka lisäksi niiden välillä kulkee Ethernet-yhteys mobiilidataa varten. (Audi of America, 2021, ss.10–11) Avaimettoman kulun ja käynnistyksen järjestelmässä J965 vastaa matalan taajuuden signaalin lähettämisestä avaimeen, ja J519 viestii avaimen kanssa korkeammilla taajuuksilla saatuaan herätteen J965:ltä.

Kartoituksessa tarkasteltiin ensin J965:n, J519:n ja avaimen lähetin-vastaanottimen yhdessä muodostaman avaimettoman kulun ja käynnistämisen järjestelmää. Selkeimpänä siihen liittyvänä riskinä pidettiin välityshyökkäystä. Sen seurauksena hyökkääjä voi varastaa auton, tai käyttää hyökkäystä keinona päästä käsiksi auton USB- tai OBD2-portteihin. Välityshyökkäyksellä arvioitiin olevan vakavia seurauksia, ja sen toteutumista pidettiin kaikista hyökkäyksistä todennäköisimpänä sen kohtuullisen yksinkertaisen toteuttamistavan ja vaaditun välineistön vuoksi. Siltä voi kuitenkin suojautua halutessaan helposti säilyttämällä auton avainta suljetussa tilassa, joka ei päästä signaalia ulkopuolelleen.

Seuraavaksi siirryttiin pohtimaan J949:n ja etenkin sen LTE-yhteyteen liittyviä riskejä. Siihen liittyen havaittiin kaksi mahdollista riskiä, man-in-the-middle-hyökkäykset ja verkon konfiguraatioon liittyvät haavoittuvuudet. Yhteinen piirre näille on se, että kuluttajan mahdollisuudet vaikuttaa niiden toteutumiseen tai seurauksiin ovat käytännössä olemattomat.

Man-in-the-middle-hyökkäyksessä hyökkääjä voi päästä seuraamaan autosta palvelimelle liikkuvaa dataa, joka voi käsittää henkilökohtaisiakin tietoja. Sen todennäköisyys arvioitiin kuitenkin matalaksi, vaikka toteutuessaan sillä voisi olla kohtuullisen ikäviä seurauksia. Autovalmistaja voi toimenpiteillään vaikuttaa seurauksien vakavuuteen salaamalla kaiken datan.

Verkon haavoittuvuuksien myötä uhkana voi olla yhteyden muodostamisen mahdollisuus samassa verkossa olevalta laitteelta, jolloin hyökkäys voi edetä myös auton sisäisiin verkkoihin auton järjestelmien haavoittuvuuksia hyödyntäen. Myös tämän riskin toteutumisen todennäköisyys arvioitiin matalaksi, mutta sen toteutumisen seurauksia pidettiin vakavina. Siksi on tärkeää, että auton valmistaja varmistaa, että verkko, johon auto on yhteydessä, on toteutettu turvallisesti estäen tällaiset hyökkäykset.

Lopuksi tutkittiin J794:n Wi-Fi- ja Bluetooth-yhteyksiin sekä USB-portteihin liittyviä riskejä. Wi-Fi-yhteyteen liittyen riskiksi arvioitiin hyökkääjän luvaton pääsy verkkoon. Se muodostaa samanlaisia uhkia, kuin LTE-verkon kautta yhteyden muodostaminen, joten myös tämän riskin toteutumisen seurauksien arvioitiin olevan vakavat. Toteutumisen todennäköisyyttä pidettiin kuitenkin matalana. Kuluttaja voi estää tällaisen hyökkäyksen uhriksi joutumisen pidättäytymällä käyttämästä Wi-Fiä.

Bluetoothiin liittyen riskinä pidettiin sen haavoittuvuuksia, joita on vuosien varrella löydetty ja korjattu usein. Hyökkääjä voi haavoittuvuuksia hyödyntäen päästä käsiksi auton tietoviihdejärjestelmään tallennettuihin tietoihin. Seuraukset ja todennäköisyys Bluetoothiin liittyvien riskien kohdalla arvioitiin melko mataliksi, ja niiltä voi välttyä esimerkiksi harkitsemalla, mitä tietoa Bluetoothin kautta autoon halua tallentaa, ja seuraamalla, onko autoon liitetty tuntemattomia laitteita.

USB-portteihin liittyviksi uhiksi arvioitiin haittaohjelmat, joita niiden kautta voidaan asentaa esimerkiksi ohjelmiston muokkaamistarkoituksessa. Riskin toteutuminen on epätodennäköistä, sillä päästäkseen käsiksi fyysisiin portteihin hyökkääjän täytyy joko saada auton käyttäjä liittämään haittaohjelman sisältävä laite porttiin, tai jollakin toisella keinolla päästävä itse auton sisälle. Toteutuessaan tällä kuitenkin voi olla vastaavat seuraukset kuin langattomiin yhteyksiin kohdistuvilla hyökkäyksillä. Kuluttaja voi ehkäistä tämän huolehtimalla, ettei liitä USB-portteihin tuntemattomia laitteita.

9.4 CAN-viestien takaisinmallintaminen ja lähettäminen

CAN-väylässä liikkuvan datan tarkkailu, kerääminen ja manipulointi suoritettiin Kali Linux 2023.4 -virtuaalikoneella auton mittaristoa simuloivaa ICSim-ohjelmistoa ja can-utils-työkaluja hyödyntäen.

Toteutusvaiheessa varmistettiin aluksi järjestelmän toimivuus ohjainta käyttäen, jonka jälkeen tallennettiin lokitiedostoon muutaman sekunnin aikana virtuaalisessa CAN-väylässä liikkunut data. Tänä aikana lukitus avattiin ja suljettiin ohjainta käyttäen. Datan tallentaminen tiedostoon käynnistettiin Komento 1. Kun tallentamisen päättää, tiedosto tallentuu automaattisesti myöhempää käyttöä varten.

Komento 1, CAN-väylän datan tallentaminen tiedostoon

```
candump -l vcan0
```

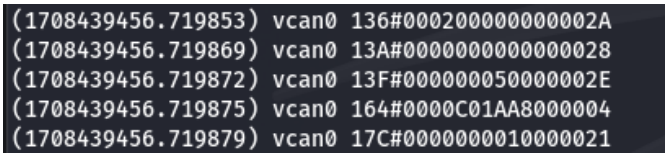
Komento 2 voidaan tarkastella tallennetun tiedoston sisältöä suoraan komentoriviltä.

Komento 2, tiedoston tarkastelu komentoriviltä

```
cat candump-2024-02-20_163056.log
```

Tiedoston rakenne havainnollistetaan Kuva 5, jossa jokainen tiedoston rivi on erillinen väylässä liikkuva viesti. Näistä suurin osa on ns. taustakohinaa, joka ei ole tutkimuksen kannalta relevanttia.

Kuva 5, tallennetun tiedoston rakenne



Työn seuraavassa vaiheessa ohjain kytkettiin pois, ja tästä eteenpäin kaikki mittaristolle siirretty data oli peräisin tallennetusta tiedostosta, jonka osia CAN-väylään syötettiin. Jakamalla tiedosto osiin, saatiin aluksi erotettua lukituksen avaava ja sulkeva viesti omiin tiedostoihinsa, jonka jälkeen keskityttiin vain toiseen näistä. Toistamalla muutamasta vaiheesta koostuvaa prosessia, jäljelle jäi lopulta yhden rivin sisältävä tiedosto, joka CAN-väylään lähetettynä avasi lukituksen. Komennot, joita prosessissa käytettiin, havainnollistetaan komennoissa Komento 3 ja Komento 4. Käytännössä prosessi koostui seuraavista vaiheista:

1. Jaa lukituksen avaavan viestin sisältävä tiedosto kahteen yhtä suureen osaan rivimäärän mukaan.
2. Lähetä tiedoston ensimmäinen puolikas CAN-väylään. Jos lukitus aukeaa, siirry vaiheeseen 4.
3. Mikäli lukitus ei aukea, lähetä tiedoston toinen puolikas varmistuaksesi, että se avaa lukituksen eikä virhettä ole tapahtunut.
4. Kun lukitus on auki, lähetä väylään tiedosto, joka sisältää lukituksen sulkevan viestin. Siirry takaisin vaiheeseen 1.

Komento 3, tiedoston jakaminen puoliksi

```
split -l 2048 canlog3aa canlog4
```

Komento 4, tiedostojen lähettäminen CAN-väylään

```
canplayer -I canlog4aa
```

```
canplayer -I canlog4ab
canplayer -I doorlock
```

Kun lukituksen avaava viesti saatiin selville, sen rakennetta tutkimalla pystyttiin selvittämään myös lukituksen sulkeva viesti. Viestit erosivat toisistaan ainoastaan yhden merkin osalta. Komentoja Komento 5 ja Komento 6 käyttäen nämä viestit voitiin syöttää CAN-väylään niiden toimivuuden varmistamiseksi.

Komento 5, ovet lukitsevan viestin lähettäminen

```
cansend vcan0 19B#00000F000000
```

Komento 6, lukituksen avaavan viestin lähettäminen

```
cansend vcan0 19B#000000000000
```

10 Johtopäätökset ja pohdinta

Tässä luvussa käydään läpi opinnäytetyöprosessi kiinnittäen huomiota siihen, millä keinoilla vastaukset tutkimuskysymyksiin löydettiin, ja tarkastellaan tutkimuksen sekä teoria- että käytännön osan tuloksia.

10.1 Opinnäytetyöprosessi

Opinnäytetyöprosessi alkoi aiheen pohtimisella, ja pyörittelin mielessäni useita vaihtoehtoja ennen lopullisen valinnan tekemistä. Ajatus oli alusta lähtien valita jokin ajankohtainen kyberturvallisuuteen liittyvä aihe, jolla olisi kohtuullisen laaja kohderyhmä. Paljon autoilevana ja autojen kehityksestä kiinnostuneena ihmisenä päädyin yhdistämään aiheessa sekä autot että kyberturvallisuuden.

Työn valmiiksi saattaminen oli yllättävän vaikeaa, vaikka tiedostin, että paljon autojen tekniikkaan liittyvää opiskeltavaa olisi luvassa. Erilaisten järjestelmien määrä ja monimutkaisuus kuitenkin yllätti, ja välillä dokumentaation heikon saatavuuden tai eri yhteyksissä käytettyjen käsitteiden tai lyhenteiden ristiriitaisuuksien vuoksi oli hankalaa edetä. Vaikeuksista huolimatta työstä kuitenkin tuli ainakin omasta mielestäni hyvä ja riittävän helposti ymmärrettävä tietopaketti aiheesta kiinnostuneelle, ja se olikin yhtenä päätavoitteena prosessin alusta alkaen.

Työssä etsittiin vastauksia kolmeen tutkimuskysymykseen, joiden pohjalta rakentuivat sekä teoria-, että käytännön osa. Ensimmäiseen kysymykseen, millaisia uhkia internetiin yhdistettyihin autoihin kohdistuu, vastaamiseksi tarvittiin laaja katsaus autoissa käytettyihin mahdollisesti haavoittuvaisiin teknologioihin. Käytännön esimerkkien ja kyberturvallisuusraporttien analysoinnin pohjalta saatiin muodostettua kokonaiskuva autoihin liittyvistä kyberuhista.

Toiseen kysymykseen, miten uhkiin on reagoitu, vastaamiseksi selvitettiin autoalan kyberturvallisuutta käsittelevien standardien ja lainsäädännön kehittymistä, ja tutustuttiin autojen kyberturvallisuuden parantamiseksi käytettyjen järjestelmien ja menetelmien toimintaan. Kolmanteen kysymykseen, miten autoilija voi torjua tai välttää uhkia, saatiin vastaus yhdistelemällä teoriaosan tietoa ja kartoittamalla auton järjestelmiin liittyviä riskejä sen pohjalta. Riskikartoituksessa kiinnitettiin erityisesti huomiota toimenpiteisiin, joilla autoilija voi torjua uhkia.

10.2 Tulokset

Työn teoriaosan tuloksena saatiin sopivan laaja katsaus työssä käsiteltävistä aiheista, jonka lukijalle se tuottaa ideaalitilanteessa reilusti uutta tietoa. Siinä perehdytään auton sisäisten tiedonsiirtoväylien toimintaan ja rakenteisiin, sekä ulkoisten yhteyksien vaikutuksesta niihin yhdistettyihin järjestelmiin kohdistuviin kyberuhkiin. Myös valmistajien keräämään dataan liittyvät riskit ja alaa koskevat standardit ja sääntely, sekä ainakin osittain niiden myötä kehittyneet turvallisuusjärjestelmät ja niiden perusperiaatteet avataan lukijalle. Teorialuvuissa käsitellyt asiat koskettavat jo nyt suurta joukkoa autoilijoita, ja tulevaisuudessa osuus tulee kasvamaan autokannan uudistuessa.

Työn käytännön osassa tutkittiin yksittäisen henkilöauton järjestelmiä, niihin liittyviä riskejä ja hyökkäyspolkuja. Riskikartoituksessa todettiin, että todennäköisimmin toteutuvat riskit ovat vaikutuksiltaan lievimpiä, ja päinvastoin. Havaittiin myös, että suurin osa järjestelmistä on varsin helposti suojattavissa autoilijan omilla toimenpiteillä. Toimenpiteet tosin vaikuttavat negatiivisesti auton modernien mukavuusvarusteiden käytettävyyteen, estäen mm. musiikin toistamisen langattomasti mobiililaitteen kautta. Siksi olisikin tärkeää, että autoteollisuus ja lainsäätäjät kiinnittäisivät erityistä huomiota langattomien yhteyksien ja auton tiedonsiirtojärjestelmien rakenteen turvallisuuteen.

Kuten myös teoriassa kävi ilmi, vakavimpien riskien toteutuessa hyökkääjä pääsee manipuloiman auton tiedonsiirtoväylissä liikkuvaa dataa. Siihen liittyen tehtiin hieman konkreettisempi koe, jossa CAN-väylän liikennettä takaisinmallinnettiin onnistuneesti ja löydettiin komennot, joilla auton ovien lukituksen toimintaan pystyttiin vaikuttamaan.

Vaikka kyse oli virtuaalisessa ympäristössä suoritetusta kokeilusta, voi sen pohjalta kuitenkin saada käsityksen siitä, miten helposti joltakulta aiheeseen perehtyneeltä tämän kaltainen toiminta todellisessa ympäristössä voi yksinkertaisimmillaan onnistua. Tämän vuoksi siis tilanteita, jossa epäystävällinen taho pääsee käsiksi CAN-väylään, kannattaa pyrkiä torjumaan erityisen tehokkaasti.

Työssä esille tulleiden seikkojen valossa voidaan todeta, että uusimmat autot, joiden suunnittelussa ja valmistuksessa on edetty standardien ja asetusten ohjaamina, ovat todennäköisesti kyberturvallisuutensa suhteen vähintään melko turvallisia. Kuluttajan kannalta tosin kokonaiskuva ei välttämättä ole lainkaan aiempaa parempi, sillä kerätty data voidaan nähdä myös riskinä.

Jos tarkastellaan tilannetta pelkästään autoilijan fyysistä turvallisuutta uhkaavien tekijöiden kannalta, vaikuttavat 2010-luvun puolivälin aikoihin markkinoille tulleet autot haavoittuvaisimmilta. Toisaalta tilanne myös niiden turvallisuuden suhteen on voinut parantua merkittävästi järjestelmäpäivitysten tai takaisinkutsujen yhteydessä suoritettujen toimenpiteiden myötä.

Työssä kävi ilmi, että kuluttajan mahdollisuudet vaikuttaa omaan kyberturvallisuuteensa rajoittuvat lähinnä auton ominaisuuksien käytöstä pidättäytymiseen. Mahdollisia kyberturvallisuusriskejä tuovat järjestelmät kuuluvat nykyisin usein auton vakiovarusteisiin. Onkin aiheellista pohtia, tulisiko valmistajien myös tarjota vähemmän varusteltuja vaihtoehtoja niistä kiinnostuneille asiakkaille.

11 Yhteenveto

Työn tutkimuskysymyksiin vastaaminen onnistui hyvin, joskin niistä viimeiseen olisin toivonut pystyväni tarjoamaan yksityiskohtaisempia vastauksia. Vaikeudeksi tässä muodostui tiedon saatavuus, sillä useimmat autovalmistajat jakavat hyvin vähän tietoa järjestelmistään julkisesti. Muihin kysymyksiin vastaukset ovat nähdäkseni tarpeeksi laajat.

Opinnäytetyön tekoa aloittaessa tietoni aiheesta rajoittuivat lähinnä kyberturvallisuuteen liittyvien perusasioiden osaamiseen, sekä joihinkin autojen hakkerointia koskeneisiin uutisiin. Siispä prosessin aikana uutta tietoa kertyi todella paljon, etenkin autojen tiedonsiirtomenetelmiin ja niiden toimintaan sekä haavoittuvuuksiin liittyen.

Autoteollisuus on kehittynyt viimeisten vuosikymmenten aikana nopeasti, ja sama kehityskulku jatkunee myös tulevaisuudessa. Tällä hetkellä todennäköiseltä vaikuttaa autojen välisen kommunikaation yleistyminen, ja esimerkiksi sen turvallisuuteen liittyen pystyisi varmasti toteuttamaan erillisen tutkimuksen, mikäli tulevaisuudessa opintojen myötä mahdollisuus tälle aukeaa.

Lähteet

Audi of America. (2.2021). *Third-generation modular infotainment matrix.* https://static.nhtsa.gov/odi/tsbs/2021/MC-10189329-0001.pdf

Autoalan Tiedotuskeskus. (12.1.2024). *Henkilöautojen ensirekisteröinnit merkeittäin 2023.* https://www.aut.fi/tilastot/ensirekisteroinnit/henkiloautojen_vuosittaiset_merkki-_ja_mallitilastot/2023/merkeittain?sort_column=1&sort_direction=1

Autocrypt. (25.3.2020). *How Do Vehicles Connect to the Internet and Why Would Someone Hack Them?* https://autocrypt.io/how-do-vehicles-connect-to-the-internet-and-why-would-someone-hack-them/

AutoPi. (16.2.2023). *Ultimate OBD2 Guide: Understanding Vehicle Diagnostics.* https://www.autopi.io/blog/what-is-obd-2/

AutoPi. (20.10.2022). *What Kind of Data Is My Vehicle Collecting?* https://www.autopi.io/blog/the-meaning-of-vehicle-data/

Bakhshiyeva, A. & Berevelt, G. (9.9.2022). *Eavesdropping Attacks on Modern Day Connected Vehicles and Their Ramifications.* https://www.diva-portal.org/smash/get/diva2:1710393/FULLTEXT01.pdf

Beaumont, S. I. (2023*). Commonalities in Vehicle Vulnerabilities.* IOActive. https://act-on.ioactive.com/acton/attachment/34793/f-74e70d46-0e06-44a6-9de5-e16b9bec4cf3/1/-/-/-/-/Commonalities-Vechicle-Vulnerabilities_22update.pdf

Becsi, T., Aradi, S. & Gaspar, P. (6.2015). *Security issues and vulnerabilities in connected car systems.* https://www.researchgate.net/publication/281447339_Security_issues_and_vulnerabilities_in_connected_car_systems

Borza, M. (19.5.2021). *Automotive Cybersecurity for ECUs & In-Vehicle Networks*. Chip Design. https://www.synopsys.com/blogs/chip-design/automotive-cybersecurity-for-ecus-in-vehicle-networks.html

Caltrider, J., Rykov, M. & MacDonald, Z. (6.9.2023). *It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy.* Mozilla Foundation. https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/

Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F. & Kohno, T. (2011). *Comprehensive Experimental Analyses of Automotive Attack Surfaces.* https://www.usenix.org/legacy/events/sec11/tech/full_papers/Checkoway.pdf

Cinch. (n.d.). *OTA updates in cars – what are over-the-air updates?* https://www.cinch.co.uk/guides/car-maintenance/over-the-air-car-updates

CISA. (27.8.2018). *Harman-Kardon Uconnect Vulnerability.* Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/ics-advisories/icsa-15-260-01

Cisco. (n.d.-a). *What Is a Cyberattack?* https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

Cisco. (n.d.-b). *What Is Cybersecurity?* https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html?dtid=osscdc000283

Compass. (n.d.). *Connected Vehicles Guide | Part 1: A Brief Background on Connected Vehicles.* https://www.compassiotglobal.com/ultimate-guide-to-connected-vehicles/part-1-background-on-connected-vehicles-and-connected-vehicle-data

Copperpod. (3.1.2022). *Evolution of Bluetooth.* https://www.copperpodip.com/post/evolution-of-bluetooth

Di Francesco, E. (16.5.2023). *The Remarkable Evolution of Car Design and Technology from 1900 to 2023.* https://mycarheaven.com/2023/05/the-remarkable-evolution-of-car-design-and-technology-from-1900-to-2023/

ENISA. (n.d.). *Man-in-the-Middle.* https://www.enisa.europa.eu/topics/incident-response/glossary/man-in-the-middle

ENISA. (13.1.2017-a). *Cyber Security and Resilience of smart cars*. Euroopan unionin verkko- ja tietoturvavirasto. https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars

ENISA. (9.2017-b). *ENISA overview of cybersecurity and related terminology.* https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology

European Commission. (n.d.). *Vehicle Safety Systems.* https://transport.ec.europa.eu/transport-themes/intelligent-transport-systems/road/application-areas/vehicle-safety-systems_en

Falch, M. (4.2022). *CAN Bus Explained - A Simple Intro [2023]*. CSS Electronics. Haettu 2.2.2024 osoitteesta https://www.csselectronics.com/pages/can-bus-simple-intro-tutorial

Francillon, A., Danev, B. & Capkun, S. (2011). *Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars*. https://doi.org/10.3929/ethz-a-006708714

Gabriel-Ionel, G. (2.10.2023). *Security In Automotive: Connected Cars, Cyber Risks, And Safeguarding The Future Of Mobility.* Stefanini Group. https://stefanini.com/en/insights/articles/security-in-automotive-industry

Goldstein, F. (3.5.2020). *ISO/SAE 21434: Setting the Standard for Automotive Cybersecurity.* Upstream. https://upstream.auto/blog/setting-the-standard-for-automotive-cybersecurity/

Gu, H. (20.7.2021). *NXP, Volkswagen and Partners Continue to Accelerate the V2X Rollout.* NXP. http://www.nxp.com/company/blog/nxp-volkswagen-and-partners-continue-to-accelerate-the-v2x-rollout:BL-THE-V2X-ROLLOUT

Huq, N., Gibson, C., Kropotov, V., Vosseler, R. (n.d.). *Cybersecurity for Connected Cars.* TrendMicro. https://resources.trendmicro.com/Cybersecurity-Connected-Cars-WP.html

Hurtado, J. (5.2023). *What are the latest automotive cybersecurity trends?* Prescouter. https://www.prescouter.com/2023/05/latest-automotive-cybersecurity-trends/

JYU. (23.4.2015). *Tapaustutkimus.* https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/tapaustutkimus

Kali Org. (n.d.). *The most advanced Penetration Testing Distribution.* https://www.kali.org/

Knight, A. (9.7.2018). *The Hitchhiker's Guide to Hacking Connected Cars: Evil Twin Attack Against a Connected Car*. Brier & Thorn. https://www.brierandthorn.com/post/the-hitchhiker-s-guide-to-hacking-connected-cars-evil-twin-attack-against-a-connected-car

Knight, A. (2020). *Hacking connected cars : Tactics, techniques, and procedures.* John Wiley & Sons, Incorporated. https://ebookcentral-proquest-com.ezproxy.hamk.fi/lib/hamk-ebooks/detail.action?docID=6119409

Kuzin, M. & Chebyshev, V. (16.2.2017*). Mobile apps and stealing a connected car.* Securelist. https://securelist.com/mobile-apps-and-stealing-a-connected-car/77576/

Lo Bello L., Patti, G. & Leonardi L. (18.1.2023). *A Perspective on Ethernet in Automotive Communications—Current Status and Future Trends*. Applied Sciences. 2023; 13(3):1278. https://doi.org/10.3390/app13031278

Mataciunas, M. (4.4.2023*). How connectivity is transforming the automotive industry*. ICA Summit. https://ica-summit.com/autonomous-and-connected-technology/how-connectivity-is-transforming-the-automotive-industry/

McGratch, D. (7.4.2020). *How 5G Changes the V2X communications game.* 5G Technology World. https://www.5gtechnologyworld.com/how-5g-changes-the-v2x-communications-game/

Meah, J. (11.7.2023*). Driving into the Future: The Latest Advances in Automotive Security.* https://www.techopedia.com/driving-into-the-future-the-latest-advances-in-automotive-security

Mertl, S. (5.3.2016). *How cars have become rolling computers*. The Globe And Mail. https://www.theglobeandmail.com/globe-drive/how-cars-have-become-rolling-computers/article29008154/

Nasr, T., Torabi, S., Bou-Harb, E. & Fachka, C. (11.2021). *Power Jacking Your Station: In-Depth Security Analysis of Electric Vehicle Charging Station Management Systems.* https://www.researchgate.net/publication/355860224_Power_Jacking_Your_Station_In-Depth_Security_Analysis_of_Electric_Vehicle_Charging_Station_Management_Systems

Newcomb, D. (25.08.2011). *Car Tech 101: Bluetooth Basics.* https://www.edmunds.com/car-technology/car-tech-101-bluetooth-basics.html

NHTSA. (2022). *Cybersecurity Best Practices for the Safety of Modern Vehicles.* National Highway Traffic Safety Administration. https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-pre-final-tag_0_0.pdf

NI, (17.11.2023). *FlexRay Automotive Communication Bus Overview*. NI. https://www.ni.com/en/shop/seamlessly-connect-to-third-party-devices-and-supervisory-system/flexray-automotive-communication-bus-overview.html

Oka, D. K. (14.6.2021). *Connected Vehicle Cybersecurity for Wireless Communications.* Chip Design. https://www.synopsys.com/blogs/chip-design/connected-vehicle-cybersecurity-wireless-comm.html

Pitchford, M. (8.8.2022). *ISO/SAE 21434: Software certification for automotive cybersecurity.* EDN. https://www.edn.com/iso-sae-21434-software-certification-for-automotive-cybersecurity/?_ga=2.34022886.696468000.1708528765-925078279.1707085832

Proofpoint. (n.d.). *Cybersecurity Vulnerabilities.* https://www.proofpoint.com/us/threat-reference/vulnerability

Riikonen, J. (20.04.2022*). Liikenteessä on jo käytössä telematiikkaa, joka mahdollistaa tulevien robottiautojen käytön*. Helsingin Sanomat. https://www.hs.fi/visio/art-2000008496779.html

Rousku, K. (02.06.2017). *Ohje Riskienhallintaan.* http://urn.fi/URN:ISBN:978-952-251-862-0

SAE International. (15.12.2021). *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems.* https://www.sae.org/standards/content/j3061_202112/

Salminen, A. (2011). *Mikä kirjallisuuskatsaus?* https://www.uwasa.fi/materiaali/pdf/isbn_978-952-476-349-3.pdf

Schmid, M. (n.d.). *Automotive bus systems.* https://user.eng.umd.edu/~austin/enes489p/project-resources/SchmidAutoBusSystems.pdf

Shechter, S. (18.10.2023). *How to mitigate vulnerabilities in keyless entry systems. Automotive World*. https://www.automotiveworld.com/articles/mitigating-vulnerabilities-in-keyless-entry-systems/

Skoda. (n.d.-a). *HENKILÖTIETOJEN SUOJAUSTA KOSKEVA LAUSUNTO.* https://www.skoda-auto.com/other/privacy-policy-fi?_gl=1*10bae8z*GA4_ga*ZjA0ZmZiZjAtYzIyZS00MjZiLWJkNzQtOGYzZjY2NTYxMzlm*GA4_ga_TE5QSWFXZT*MTcwODI3OTQ1NS4xLjEuMTcwODI3OTY5Ni4wLjAuMA..*_gcl_au*Mjk1MjQ5ODQ1LjE3MDgyNzk0NTU.

Skoda. (n.d.-b). *Tietosuojailmoitus.* https://skodaid.vwgroup.io/data-privacy

Skoda Storyboard. (29.06.2020). *ŠKODA KAROQ, KODIAQ and SUPERB begin 2021 model year with new infotainment generation.* https://www.skoda-storyboard.com/en/press-releases/skoda-karoq-kodiaq-and-superb-begin-2021-model-year-with-new-infotainment-generation/

Smith, C. (2016). *The Car Hacker's Handbook: A Guide for the Penetration Tester*. No Starch Press, Incorporated, San Francisco. https://ebookcentral-proquest-com.ezproxy.hamk.fi/lib/hamk-ebooks/detail.action?docID=4503176

Spaar, D. & Scherschel F. A. (5.2.2015) *Beemer, Open Thyself! – Security vulnerabilities in BMW's ConnectedDrive.* Heise Online. https://www.heise.de/hintergrund/Beemer-Open-Thyself-2540957.html

SSH. (n.d.). *What is PKI (Public Key Infrastructure)?* https://www.ssh.com/academy/pki

Stevens, T. (5.9.2023). *How Is All the Data in Your Car Being Protected?* https://www.motortrend.com/features/car-data-security-protection/

Strzalkowski, P. (30.3.2023). *R155/R156 - a quick guide to the updated cybersecurity regulations for automotive.* Solw'IT. https://solwit.com/en/blog/r155-r156-a-quick-guide-to-the-updated-cybersecurity-regulations-for-automotive/

TechSparks (15.10.2023*). What Is an Electronic Control Unit (ECU) and How It Work*. https://www.tech-sparks.com/electronic-control-unit/

Tesla (1.2024). *Asiakkaan Tietosuojailmoitus.* Haettu 18.2.2024 osoitteesta https://www.tesla.com/fi_fi/legal/privacy

Toulas, B. (1.12.2022). *Hyundai app bugs allowed hackers to remotely unlock, start cars.* https://www.bleepingcomputer.com/news/security/hyundai-app-bugs-allowed-hackers-to-remotely-unlock-start-cars/

UNECE. (2021-a). *UN Regulation No. 155 - Cyber security and cyber security management system.* https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security

UNECE. (2021-b). *UN Regulation No. 156 - Software update and software update management system.* https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update

Ungurean, M.C. (n.d.). *Cybersecurity in Automotive: Current Trends, Regulations, and Future Paths.* Rinf.tech. https://www.rinf.tech/cybersecurity-in-automotive-current-trends-regulations-future-paths/

Upstream. (2023). *Global Automotive Cybersecurity Report 2023.* Ladattavissa https://upstream.auto/reports/2023report/

Valasek, C. & Miller, C. (2015*). Remote Exploitation of an Unaltered Passenger Vehicle.* https://ioactive.com/pdfs/IOActive_Remote_Car_Hacking.pdf

Vector. (n.d.). *Automotive Intrusion Detection Systems.* https://www.vector.com/int/en/know-how/security/automotive-intrusion-detection-systems/#

Venkat, S. (11.2020*). Evolving Automotive Gateways for Next-Generation Vehicles*. https://www.ti.com/lit/pdf/spry333?keyMatch=EVOLVING%20AUTOMOTIVE%20GATEWAYS%20FOR%20NEXT-GENERATION%20VEHICLES

Volvo. (9.10.2023). *Volvo-autojen Tietosuojailmoitus.* Haettu 18.2.2024 osoitteesta https://www.volvocars.com/fi/legal/privacy/privacy-car#c87fad66941db53cc0a8015130d4f196

Volvo. (15.1.2024-a). *Tietosuojailmoitus – Volvo Cars -sovellus.* Haettu 18.2.2024 osoitteesta https://www.volvocars.com/fi/legal/privacy/privacy-voc#41b2dae64460d4f8c0a800650811c1a3

Volvo. (15.1.2024-b). *Volvo Carsin yleinen tietosuojailmoitus.* Haettu 18.2.2024 osoitteesta https://www.volvocars.com/fi/legal/privacy/privacy-customer-privacy-policy#39e73983bd6f22cfc0a801512f1f7a97

Williams, M. (30.1.2015) *BMW cars found vulnerable in Connected Drive hack.* PCWorld. https://www.pcworld.com/article/431610/bmw-cars-found-vulnerable-in-connected-drive-hack.html

Wolbert, D. (24.9.2021). *Everything you need to know about telematics*. Hologram. https://www.hologram.io/blog/what-is-telematics/

Liite 1: Aineistonhallintasuunnitelma

Tutkimuksellinen työ:

Työn aineisto ei sisällä henkilötietoja, joten tarvetta anonymisoinnille ei ole. Kaikki kerätty aineisto tallennetaan sekä työn tekijän tietokoneen C-asemalle, että ulkoiseen pilvitallennustilaan. Varmuuskopioita aineistosta tehdään työn aikana säännöllisesti Google Driveen. Aineistoa säilytetään ainakin vuoden ajan opinnäytetyön valmistumisen jälkeen. Aineistoon pääsee käsiksi ainoastaan opinnäytetyön tekijä.

Opinnäytetyöaineiston jatkokäyttö työn valmistumisen jälkeen

1. Et halua hyödyntää tai antaa tutkimusaineistoasi jatkokäyttöön

Tutkimusaineistoa ei jatkokäytetä. Opinnäytetyön tekijä säilyttää aineiston tietoturvallisesti vuoden ajan opinnäytetyön hyväksymispäivästä, jotta opinnäytetyön tulokset voidaan tarvittaessa varmistaa ja hävittää tämän jälkeen aineiston tietoturvallisesti.

Liite 2. Riskikartoitus

Laite	Suojattava yhteys/portti	Uhka	Vaikutus	Vaikutus (1-4)	Todennäköisyys (1-4)	Kriittisyys (vaikutus * todennäköisyys)
J965 (Interface for entry and start system), J519 (Onboard supply control unit) & avaimen lähetin-vastaanotin	LF- ja UHF-yhteys	Välityshyökkäys (relay attack)	Pääsy auton sisälle, mahdollisuus käynnistää auto ja ajaa sillä. Pääsy USB/OBD2-portteihin, ja näiden kautta tiedonsiirtoväyliin. Lisäksi pääsy auton tietoviihdejärjestelmän tallennettuihin tietoihin, kuten yhteystietoihin, osoitteisiin ja tekstiviesteihin.	3	3	9
J949 (Emergency call module control unit and communication unit)	LTE	Luvaton yhteys kohdelaitteeseen	Hyökkääjä voi päästä syöttämään dataa J949:n CAN-väylään ja vaikuttaa siten väylän ECUjen toimintaan. Väylän ECUt ohjaavat mm. mittaristoa, vakionopeudensäädintä ja ilmastointia. Mahdollisesti avaa myös yhdyskäytävän kautta pääsyn muihin väyliin.	4	1	4
	LTE	Man in the middle -hyökkäys (esim. rogue BTS)	Auton ja palvelimen välistä liikennettä päästään tarkkailemaan.	3	2	6
J794 (Control unit 1 for infotainment electronics)	USB	Haittaohjelmat	Muokatun ohjelmistoversion asentamalla hyökkääjä voi mahdollisesti esim. päästä kirjautumaan järjestelmään pääkäyttäjänä ja ottaa käyttöön sshd:n mahdollistaakseen etäyhteyden muodostamisen järjestelmään tulevaisuudessa.	4	1	4
	Bluetooth	Haavoittuvuudet	Hyökkääjä saa pääsyn auton järjestelmiin tallennettuihin tietoihin, esim. yhteystiedot tai tekstiviestit	2	1	2
	Wi-Fi	Luvaton yhteys (avoimet portit)	Hyökkääjä voi päästä syöttämään dataa J794:n CAN-väylään ja vaikuttaa siten väylän ECUjen toimintaan. Väylän ECUt ohjaavat tietoviihdejärjestelmän toimintaa. Mahdollisesti avaa myös yhdyskäytävän kautta pääsyn muihin väyliin.	4	1	4
	Wi-Fi	Luvaton yhteys (salasanan murtaminen)	Hyökkääjä voi päästä syöttämään dataa J794:n CAN-väylään ja vaikuttaa siten väylän ECUjen toimintaan. Väylän ECUt ohjaavat tietoviihdejärjestelmän toimintaa. Mahdollisesti avaa myös yhdyskäytävän kautta pääsyn muihin väyliin.	4	1	4

Laite	Suojattava yhteys/portti	Toimenpiteet (autoilija)	Toimenpiteet (valmistaja)
J965 (Interface for entry and start system), J519 (Onboard supply control unit) & avaimen lähetin-vastaanotin	LF- ja UHF-yhteys	Kuluttaja voi välttyä hyökkäyksen uhriksi joutumiselta suojaamalla avaimen säilyttämällä sitä esim. metallilaatikossa, joka estää signaalin pääsemisen laatikon ulkopuolelle.	Valmistajan tulisi sisällyttää avaimeen liiketunnistin, joka sopivan ajan kuluessa deaktivoi avaimen kunnes sitä liikutetaan uudestaan, tai luoda järjestelmään aikakatkaisu joka tunnistaa liian kaukaa tulevan signaalin.
J949 (Emergency call module control unit and communication unit)	LTE	Kuluttajan mahdollisuudet vaikuttaa olemattomat, teoriassa laitteen voi poistaa käytöstä ja siten katkaista yhteyden.	Valmistajan ja verkko-operaattorin yhteistyö yhteyksien suojaamiseksi on tärkeää. Auton sisäisten yhteyksien eristäminen siten, että laitteiden välistä kommunikointia rajoitetaan, on hyvä käytäntö seurausten lieventämiseksi.
	LTE	Kuluttajan mahdollisuudet vaikuttaa olemattomat, teoriassa laitteen voi poistaa käytöstä ja siten katkaista yhteyden.	Valmistaja voi esim. PKI:n käytöllä estää tällaisen hyökkäyksen haitalliset seuraukset.
J794 (Control unit 1 for infotainment electronics)	USB	Kuluttajan tulee huolehtia siitä, ettei liitä auton USB-portteihin tuntemattomia laitteita.	Valmistajan tulisi toimenpiteillään estää muokattujen päivitystiedostojen asentaminen.
	Bluetooth	Kuluttaja voi valinnoillaan jättää tallentamatta tiedot auton muistiin.	Valmistajan tulee seurata tilannetta ja tarjota päivityksiä jos Bluetoothiin liittyviä haavoittuvuuksia ilmenee
	Wi-Fi	Helpoin tapa estää hyökkäys on pidättäytyä käyttämästä Wi-Fiä.	Valmistajan tulisi huolehtia reitittimen konfiguroinnista siten, että ulkopuolinen taho ei pysty muodostamaan yhteyttä siihen. Lisäksi auton sisäisten yhteyksien eristäminen siten, että laitteiden välistä kommunikointia rajoitetaan, on hyvä käytäntö seurauksien lieventämiseksi.
	Wi-Fi	Uhriksi joutumiselta voi välttyä huolehtimalla vahvasta salasanasta, jota päivittää riittävän usein. Helpoin tapa estää hyökkäys on pidättäytyä käyttämästä Wi-Fiä.	Valmistajan tulisi huolehtia vahvasta salasanasta ja sen luomiseen käytetyn menetelmän turvallisuudesta. Lisäksi auton sisäisten yhteyksien eristäminen siten, että laitteiden välistä kommunikointia rajoitetaan, on hyvä käytäntö seurauksien lieventämiseksi.