**Niko Muukkonen**

# Itseohjautuvien ajoneuvojen kyberturvahaavoittuvuudet

Tietotekniikan kandidaatintutkielma

20. toukokuuta 2019

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

**Tekijä:** Niko Muukkonen

**Yhteystiedot:** niko.t.muukkonen@student.jyu.fi

**Työn nimi:** Itseohjautuvien ajoneuvojen kyberturvahaavoittuvuudet

**Title in English:** Cybersecurity vulnerabilities of self driving vehicles

**Työ:** Kandidaatintutkielma

**Sivumäärä:** 22+0

**Tiivistelmä:** Itseohjautuvat ajoneuvot ovat ajankohtainen aihe nykyajan liikenteen kehityksessä. Näiden ajoneuvojen kehityksessä on tärkeää ottaa huomioon kyberturvallisuus. Tämä tutkielma on pienimuotoinen kirjallisuuskatsaus, jossa käydään läpi itseohjautuvien ajoneuvojen teknologioita ja näistä teknologioista, sekä muista syistä aiheutuvia mahdollisia kyberturvahaavoittuvuuksia, joita itseohjautuvien ajoneuvojen kehityksessä voi kohdata. Tutkielmassa havaitaan kyberturvallisen itseohjautuvan ajoneuvon saavuttamisen olevan hankalaa, sillä itseohjautuvat ajoneuvot käyttävät usein monia eri teknologioita, joissa voi olla haavoittuvuuksia. Huomataan myös, että teknologioiden kyberturvallisuus ei riitä, vaan ajoneuvon käyttäjän kouluttaminen on myös tärkeää esimerkiksi käyttäjän manipuloinnin estämiseksi.

**Avainsanat:** kyberturvallisuus, itseohjautuva ajoneuvo, haavoittuvuus, haittaohjelma, käyttäjän manipulointi

**Abstract:** Self driving vehicles are a current topic in development of modern transport. Cybersecurity is a key part in developing these vehicles. This bachelors thesis is a small-scale literature review that undergoes the technologies used in self driving vehicles and the possible cybersecurity vulnerabilities caused by these technologies and other factors. We find that developing a cybersecure self driving vehicle is difficult because they use many different technologies which could have cybersecurity vulnerabilities in them. We also notice that cybersecurity of these technologies is not enough in itself. Training of the vehicle user is also important because of other cybersecurity aspects, for example social engineering.

**Keywords:** cybersecurity, self driving vehicle, vulnerability, malware, social engineering

# Kuviot

# Sisältö

# 1 Johdanto

Itseohjautuvat ajoneuvot alkavat olla todella ajankohtainen aihe ja tällaisten ajoneuvojen käyttö tulee varmasti yleistymään tulevaisuudessa. Itseohjautuvia ajoneuvoja onkin kehitteillä jo jatkuvasti monen eri ajoneuvovalmistajan ja teknologiayrityksen toimesta. Myös monet tutkimusprojektit ovat sekä edistäneet itseohjautuvien ajoneuvojen teknologiakehitystä, että tuottaneet kokeellisia ajoneuvojen automaatiototeutuksia. Nämä tutkimukset ovat johtaneet moniin eri demonstraatioihin itseohjautuvien ajoneuvojen toiminnasta ympäri maailman (Petit ja Shladover 2014, s. 546).

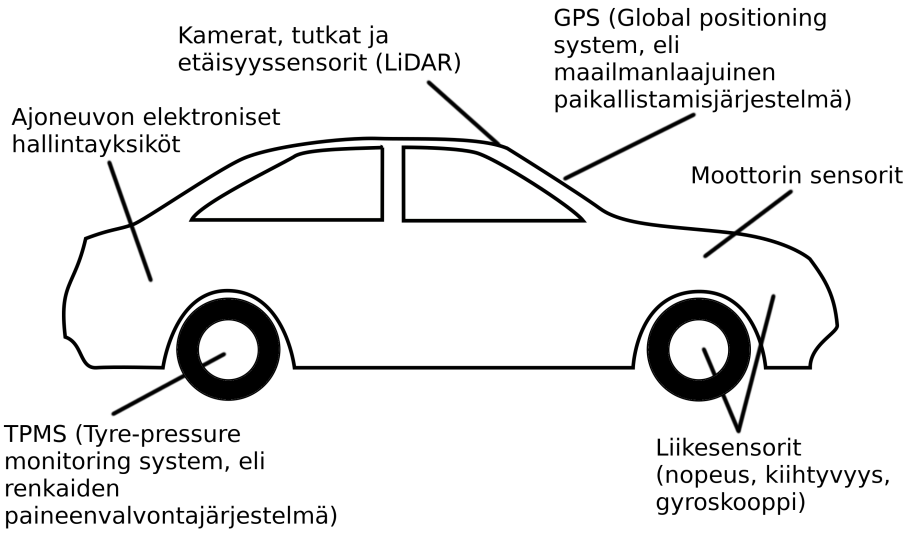
Esimerkiksi Googlen viimeaikainen kehitys itseohjautuvissa ajoneuvoissa on herättänyt laajaa mielenkiintoa mediassa ja median kiinnostuksen myötä myös huoli ja keskustelu itseohjautuvien ajoneuvojen turvallisuudesta on herännyt (Petit ja Shladover 2014, s. 546). Parkinsonin ym. (2017, s. 2898) mukaan automaation ja tietokoneiden lisääminen ajoneuvoihin ja niiden toimintaan lisääkin näiden alttiutta haavoittuvuuksille, joka saattaa lisätä näiden hyökkäysten määrää tulevaisuudessa. Petitin ja Shladoverin (2014, s. 546) mukaan myös ajoneuvoalalla on herännyt huoli muiden ajoneuvojen ja infrastruktuurin kanssa yhteydessä olevien ajoneuvojen kyberturvallisuusriskeistä ja niiden vaikutuksesta turvallisuudelle kriittisiin, kuten törmäyksen välttämiseen pyrkiviin järjestelmiin. Heidän mukaansa näiden järjestelmien kyberuhkien tunnistaminen ja niiltä suojautuminen on aihe, joka on alettu ottaa mukaan osaksi tällaisten ajoneuvojen järjestelmien tutkimusta.

Tämä tutkielma on kirjallisuuskatsaus, jonka tavoitteena on selvittää itseohjautuvien ajoneuvojen kyberturvallisuutta ja kyberturvahaavoittuvuuksia, sekä tuoda esille yksittäisiä kyberturvallisuuden kannalta tärkeitä kehityskohteita, joihin tulisi kiinnittä huomiota itseohjautuvien ajoneuvojen tukimuksessa, kehityksessä ja käytössä. Tutkielma keskittyy täysin itseohjautuviin ajoneuvoihin (full automation eli täysi automaatio). Määritelmä täydelle automaatiolle on ”Autonomisen ajojärjestelmän ehdoton täysiaikainen kaikkien dynaamisen ajotehtävän osa-alueiden suoritus kaikilla keli- ja tieolosuhteilla, jotka ihminen pystyisi hallitsemaan”, kuten SAE J3016-standardi (2014) sanoo Petitin ja Shladoverin (2014) mukaan (suomennos minun).

Luvussa 2 käsitellään itseohjautuvien ajoneuvojen sisäisiä teknologioita, kuten kameroita ja sensoreita, kerrotaan näiden teknologioiden toimintatavoista, sekä esitellään näihin teknologioihin liittyviä haavoittuvuuksia. Haittaohjelmista ja ajoneuvojen yhteyksistä muihin laitteisiin, sekä näiden aiheuttamista haavoittuvuuksista kerrotaan luvussa 3. Samassa luvussa kerrotaan myös käyttäjän manipuloinnista.

# 2 Ajoneuvon sisäiset teknologiat

Itseohjautuvat ajoneuvot käyttävät useita eri teknologioita yhdessä muodostaakseen luotettavan yleisen kuvan ajoneuvon tilasta. Kyberturvallisuuden kannalta onkin hyödyllistä käyttää dataa useasta (yli kolmesta) eri lähteestä, jotta mahdollinen virheellinen data voidaan helposti tunnistaa ja eristää järjestelmästä (Petit ja Shladover 2014, s. 551).




Kuvio 1. Yleiskuva itseohjautuvien ajoneuvojen sisäisistä teknologioista Parkinsonin ym. mukaan (2017, s. 2899-2903).

Kuten kuviossa 1 nähdään, itseohjautuvissa ajoneuvoissa on paljon sisäisiä teknologioita, joita se käyttää toimiakseen. Yksi tärkeä osa ajoneuvojen saamasta datasta muodostuu näihin sisäisiin teknologioihin kuuluvista sensoreista, kameroista ja paikannuslaitteista. Ajoneuvon sisäisiin teknologioihin kuuluvat hallintayksiköt käyttävät tätä dataa yhdessä ulkopuolelta saadun datan kanssa ajoneuvon tilan tunnistamiseen ja ajoneuvon ohjaamiseen sen perusteella.

## 2.1 GPS ja kartat

GPS (*Global positioning system*, eli maailmanlaajuinen paikallistamisjärjestelmä) on tärkeä tiedonlähde itseohjautuville ajoneuvoille. Sen avulla ajoneuvo voidaan paikantaa jopa metrin

tarkkuudella kartalle, ja sijaintitietoa hyödyntäen voidaan kartan avulla saada dataa esimerkiksi tien jyrkkyydestä (Parkinson ym. 2017, s. 2899 ja 2901). Ajoneuvossa valmiiksi olevilla kartoilla voidaan myös antaa liikkumisohjeita kartan pitkittäis- ja poikittaissuunnissa (Petit ja Shladover 2014, s. 551).

Petitin ja Shladoverin (2014, s. 551) mukaan GPS-järjestelmät ovat häirittävissä ja huijattavissa (*GPS-jamming & spoofing*) todella helposti ja edullisesti, esimerkiksi häirintälaitteita saa ostettua heidän mukaansa n. 20:llä Yhdysvaltain dollarilla. GPS-häirintä on myös heidän mukaansa myös vaikeasti havaittavissa, sillä GPS-signaalien menettäminen ei ole erikoista esimerkiksi ympäristösyistä ja näistä syistä he luokittelevatkin GPS-häirinnän korkeaksi uhkaksi. On kuitenkin hyvä huomata, että GPS-järjestelmän antama data on vain yksi datanlähde muiden joukossa, joten virheellinen data voidaan helposti jättää huomiotta, jos virhe datassa havaitaan.

Karttojen myrkyttäminen (*engl. map poisoning*) on tapa muuttaa ajoneuvojen käyttämien karttojen dataa niin, että kartat näyttävät erilaiselta, kuin pitäisi. Jeske (2013) osoitti demonstraatiossaan, miten hyökkääjät voivat ottaa haltuun ja hallita navigointijärjestelmiä ja näiden järjestelmien liikennetietoja. Itseohjautuvien ajoneuvojen näkökulmasta tämä on suuri riski, sillä ne luottavat karttojen dataan navigoidakseen. Itseohjautuvien ajoneuvojen kartat tulisikin varmentaa, eikä ulkopuoliseen dataan kuuluisi luottaa (Petit ja Shladover 2014, s. 552).

## 2.2 Esteiden tunnistus

Kameroita käytetään itseohjautuvissa ajoneuvoissa esineiden ja esteiden tunnistamiseen. Syvyyden tunnistamiseksi voidaan käyttää myös useampaa kameraa yhdessä, jolloin kahden kameran kuvien leikkauksesta voidaan muodostaa stereokuvaa. (Parkinson ym. 2017, s. 2902). Kameroiden toimintaa on kuitenkin helppo häiritä esmierkiksi sokaisemalla ne kirkkailla infrapuna LED-valoilla. Näitä LED-valoja voi Petitin ja Shladoverin (2014, s. 551) mukaan ostaa todella edullisesti (0.75 Yhdysvaltain dollaria/kappale). Sokaisemiselta suojautumiskeinona infrapunavaloa on mahdollista suodattaa sen aallonpituuden perusteella, mutta tämäkin voidaan ohittaa käyttämällä lasereita, jotka voivat vaihdella aallonpituutta (Petit ja

Shladover 2014, s. 551).

Tutkat ovat aktiivisia järjestelmiä, jotka havaitsevat esineitä lähettämällä ja vastaanottamalla radioaaltoja. Yksi tutkiin kohdistuva hyökkäys on haamuajoneuvot, eli ajoneuvot joihin on asennettu signaalintoistojärjestelmä *(DRFM, digital radio frequency memory)*. Nämä järjestelmät tallentavat digitaalisesti tutkan lähettämää radioaaltoa ja voivat lähettää sitä eteenpäin. Koska toistettu signaali on yhtenäistä signaalin lähetäneeseen tutkaan, ei tutka osaa erottaa tätä mitenkään omasta lähettämästään signaalista. (Petit ja Shladover 2014, s. 551-552).

*LiDAR* (*Light Detection and Ranging*) on puolestaan optinen tutka, joka toimii käyttäen näkyvää tai infrapunavaloa radioaaltojen sijaan (Petit ja Shladover 2014, s. 551). LiDAR:in huijaaminen ja häirintä on mahdollista käyttämällä aallonpituuksia, joita nämä järjestelmät käyttävät. Parkinson ym. (2017, s. 2902) mainitsee useita tutkimuksia joissa LiDAR:in signaalia on onnistuttu huijaamaan edullisilla keinoilla heijastamalla takaisin LiDAR:in sensoriin saman aallonpituuden valoa, jota LiDAR lähettää.

Kameroiden dataa yleensä yhdistetään muihin järjestelmiin, kuten *LiDAR*:iin tai tutkajärjestelmiin paremman esteiden tunnistamisen saavuttamiseksi. (Parkinson ym. 2017, s. 2902). Tämä on myös kyberturvallisuuden kannalta hyvä idea, koska käyttämällä useaa dataa voidaan esimerkiksi kameran häiritseminen jättää huomiotta. Itseohjautuville ajoneuvoille on kuitenkin tärkeää, että jonkinlainen esteen tunnistus on jatkuvasti toiminnassa, jotta törmäykset voidaan välttää. Järjestelmiä kehitettäessä tulisi miettiä myös tilannetta, jossa hyökkääjä pystyy häiritsemään kaikkia esteen tunnistamiseen tarjoitettuja järjestelmiä. Ajoneuvon tulisi osata pysähtyä turvallisesti jonkun muun teknologian avulla, jotta törmäykseltä vältyttäisiin.

## 2.3 Muut sensorit

Ajoneuvoissa on Petitin ja Shladoverin mukaan (2014, s. 551) lisäksi myös muita sensoreita, joista se saa dataa ajoneuvon tilan tarkkailua varten. Akustiset sensorit voivat tunnistaa tunnettuja ääniä havaitakseen esimerkiksi törmäystilanteita turvatyynysensoreita nopeammin ja laukaistakseen turvatyynyt aikaisemmin. Liikesensoreita, kuten kiihtyvyyssensoreita ja gyroskooppeja käytetään ajoneuvon liikkeen ja sen muutoksen tunnistamiseen.

Kuviossa 1 on näkyvissä renkaiden paineenvalvontajärjestelmä, joka on yksi esimerkki sensoreista, joita käytetään nykyään jo normaaleissa ajoneuvoissa itseohjautuvien ajoneuvojen lisäksi. Zhangin ym. (2014, s. 10) mukaan tutkijat ja harrastelijat ovat onnistuneet jo murtamaan renkaiden paineenvalvontajärjestelmiä, joka voi nykyajoneuvoissa johtaa kuskin uskomaan, että rengas olisi tyhjä, vaikka vikaa ei oikeasti olisi. Tälläinen haavoittuvuus voi itseohjautuvissa ajoneuvoissa johtaa myös siihen, että ajoneuvo lakkaa toimimasta ja suorittaa hallitun pysähdyksen, koska ajoneuvon tekoäly tulkitsee renkaiden olevan tyhjiä. Itsessään tämä ei aiheuta varsinaista riskiä käyttäjälle, enemmänkin vain turhaa vaivaa. Toki renkaiden painoonvalvonnan murtaminen voi aiheuttaa itseohjautuvissa ajoneuvoissa myös päinvastaisen ilmiön. Jos rengas on oikeasti puhjennut, ja paineenvalvontajärjestelmä ei annakaan tekoälylle oikeaa dataa renkaan tyhjenemisestä, tekoäly voi ajatella kaiken olevan hyvin aiheuttaen näin riskitilanteen myös ajoneuvon käyttäjälle.

Renkaiden paineenvalvontajärjestelmän sensorit ovat yksi esimerkki sensorista, jotka saattavat olla olla langattomasti yhteydessä itse ajoneuvoon. Langaton yhteys ajoneuvon ja sensorin välillä luo myös kyberturvallisuusriskin, sillä tätä langatonta signaalia voidaan häiritä tai huijata (Parkinson ym. 2017, s. 2910).

## 2.4 Ohjausjärjestelmät

Nykyaikaisissa ajoneuvoissa käytetään elektronisia ohjausjärjestelmiä, eivätkä itseohjautuvat ajoneuvot ole poikkeus. Itseohjautuvissa ajoneuvoissa näiden ohjausjärestelmien määrä on vielä suurempi kuin perinteisissä ajoneuvoissa johtuen sensoreiden ja muiden laitteiden suuremmasta määrästä perinteisiin ajoneuvoihin verrattuna (Parkinson ym. 2017, s. 2903).

Ohjausjärjestelmät ohjaavat ajoneuvon eri toimintoja ja ne voidaan jakaa Parkinsonin ym. (2017, s. 2903) mukaan neljään kategoriaan, joita ovat:

1. Voimansiirron hallinta – käsittelee ajoneuvon latausjärjestelmiä, vaihteistoa, päästöjä ja moottoria
2. Turvallisuusjärjestelmät – käsittelevät törmäyksen välttämisjärjestelmiä, turvatyynyjen toimintaa ja aktiivista jarrutusta
3. Apulaitteiden hallinta – käsittelee sähköikkunoita, peilejä, ilmastointia, ajonestolaitet-

ta ja ajoneuvon lukitusta

4. Tietoliikenteen hallinta – käsittelee tietoliikennettä eri laitteiden välillä, kuten bluetooth-yhteyttä esimerkiksi puhelimeen

Jokainen näistä ohjausjärjestelmistä on tärkeä suojata kyberturvallisuuden kannalta, koska ne ohjaavat myös ajoneuvoille ja sen käyttäjän turvallisuudelle kriittisiä toimintoja. Tietoliikenteen hallintayksikön aiheuttamista haavoittuvuuksista kerrotaan enemmän luvussa 3.

# 3 Haittaohjelmat ja yhteys muihin laitteisiin

Ajoneuvon tietoliikenteeseen keskittyvät hallintayksiköt kommunikoivat muiden ajoneuvojen, laitteiden ja infrastuktuurin kanssa eri tavoin. Yhteystapoja ajoneuvoon on monia, esimerkiksi langaton yhteys Bluetoothilla tai fyysinen yhteys USB:llä puhelimeen tai muuhun käyttäjän laitteessen, sulautettu matkapuhelinverkkojärjestelmä (*engl. Embedded cellular module*), langattoman lähiverkon yhteyspiste (*engl. Wi-Fi hotspot*) ja lyhyen kantaman tiedonsiirto (*engl. DSRC, Dedicated Short Range Communication*). Jokaisella yksiköllään on omanlaisensa yhteystapa, joten jokainen yhteysrajapinta olisi suojattava erikseen. Tämä puolestaan johtaa siihen, että yhdessä ajoneuvossa on useita suojausjärjestelmiä joista osa saattaa olla keskenään duplikaatteja (Zhang, Antunes ja Aggarwal 2014, s. 11).

On kuitenkin tärkeää huomata, että yksikin huonosti suojattu yhteystapa ajoneuvossa saattaa vaarantaa koko järjestelmän turvallisuuden, jos yhteys sisäisten laitteiden välillä ei ole suojattu tai eroteltu. Fyysistä laitteiden erottamista onkin käytetty yhtenä keinona suojata yksittäisiä järjestelmiä ajoneuvoissa (Zhang, Antunes ja Aggarwal 2014, s. 14). Tämä keino kuitenkin perustuu siihen, että erilaisten järjestelmien ei tarvitse keskustella keskenään, joten itseohjautuvien ajoneuvojen tapauksessa keinoa ei voi hyödyntää merkittävästi, sillä ajoneuvo tarvitsee tietoa monesta eri lähteestä.

## 3.1 Haittaohjelmat yleisesti

Zhangin, Antunesin ja Aggarwalin (2014, s. 10-12) mukaan haittaohjelma on käyttäjälle haitallinen ohjelma, jolla pyritään häiritsemään käyttäjän tietokonetta tai saavuttamaan luvattoman pääsyn siihen. Heidän mukaan haittaohjelmia esiintyy monissa eri muodoissa. Näitä esiintymismuotoja ovat muunmuassa:

1. Virus: Virus on haitallinen ohjelma, joka leviää toisiin tietokoneisiin ja tiedostoihin. Viruksen aktivoituessa se yrittää saastuttaa muita ohjelmia ja tietokoneita. Jokainen saastutettu ohjelma tai tietokone yrittää saastuttaa aina edelleen uusia tietokoneita ja ohjelmia.
2. Mato (*engl. Worm*): Mato on haitallinen ohjelma, joka leviää tietokoneesta toiseen

ilman, että sen tarvitsee saastuttaa erillisiä ohjelmia.

3. Troijalainen (*engl. Trojan horse*): Troijalainen on haitallinen sovellus, joka yrittää saada luvattoman pääsyn tietokoneeseen ja sen tiedostoihin näyttäessään käyttäjälle normaalilta käytettävältä ohjelmalta.
4. Vakoiluohjelma (*engl. Spyware*): Vakoiluohjelma on haitallinen ohjelma, joka kerää tietoa tietokoneesta ja lähettää sitä eteenpäin käyttäjän tietämättä.
5. Kiristysohjelma (*engl. Ransomware*): Kiristysohjelma on haitallinen ohjelma, joka rajoittaa käyttäjän pääsyn tiedostoihin vaatien lunnaita rajoituksen poistamiseksi.
6. Piilohallintaohjelma (*engl. Rootkit*): Piilohallintaohjelma on ohjelma, joka yrittää pilottaa haittaohjelmien olemassaolon tietokoneessa esimerkiksi naamioimalla haittaohjelma joksikin tärkeäksi ohjelmaksi, jotta haittaohjelman tunnistusjärjestelmät eivät tunnistaisi sitä. Piilohallintaohjelmat ovat vaikeita havaita ja poistaa, ja vaativatkin usein järjetelmän uudelleenasennuksen tai jopa jonkun fyysisen laitteen vaihtamisen sen poistamiseksi.

Välttyäkseen paljastumiselta monet nykyiset haittaohjelmat voivat muuttaa itseään jokaisella kerralla, kun ne leviävät uuteen laitteeseen tai ohjelmaan (Zhang, Antunes ja Aggarwal 2014, s. 11). Tälläisiä haittaohjelmia ovat:

1. Polymorfinen eli monimuotoinen haittaohjelma (*engl. Polymorphic malware*): Haittaohjelma, joka sisältää jokaisella muutoksella saman haitallisen koodin ja muuttuvan koodin salauksen. Jokaisella uudella muutoksella salaus on erilainen, joten ohjelma näyttää erilaiselta edelliseen verrattuna, mutta tutkittessa voidaan havaita haitallisen koodin olevan sama kuin edellisessä.
2. Metamorfinen haittaohjelma (*engl. Metamorphic malware*): Haittaohjelma joka käyttää koodin evoluutioteknologioita muuttaakseen koodin ulkomuotoa edelliseen verrattuna, jolloin myöskään haitallinen koodi ei näytä samalta edelliseen verrattuna, kuten polymorfisessa haittaohjelmassa.

Haittaohjelman pääsy tietokoneeseen on mahdollista monien eri väylien kautta, mutta vaikka haittaohjelma olisi tietokoneessa, se ei välttämättä aiheuta harmia tietokoneelle. Harmin aiheuttamiseksi haittaohjelma täytyy suorittaa tietokoneessa jollain tavalla. Suorittaminen voi

tapahtua (tahattomasti) käyttäjän toimesta tai niin kutsutun takaoven, eli järjestelmässä jo olevan tai haittaohjelman asentaman haavoittuvuuden kautta. Joskus järjestelmien kehittäjät myös jättävät näitä takaovia järjestelmiin tarkoituksellisesti helpottaakseen esimerkiksi teknistä tukea (Zhang, Antunes ja Aggarwal 2014, s. 11).

## 3.2 Haittaohjelmat itseohjautuvissa ajoneuvoissa

Haittaohjelman pääseminen itseohjautuviin ajoneuvoihin on mahdollista monen erilaisen fyysisen tai langattoman väylän kautta. Kaikissa nykyisissä ajoneuvoissa on ajoneuvon sisäinen vianmääritysjärjestelmä (*OBD, Onboard diagnostic port*). Tämä järjestelmä on ensisijaisesti tarkoitettu auttamaan ajoneuvon korjauksessa, huollossa ja katsastuksessa, mutta se antaa myös väylän päästä käsiksi ajoneuvon sisäisiin verkkoihin ja elektronisiin järjestelmiin (Zhang, Antunes ja Aggarwal 2014, s. 12). Koska tämä väylä antaa helpon pääsyn sisäisiin järjestelmiin, saattaa väylä olla riski myös kyberturvallisuuden kannalta. Tätä riskiä kuitenkin lieventää se, että vianmääritysjärjestelmään käsiksi pääseminen vaatii käytännössä ulkoisen fyysisen laitteen asentamista ajoneuvon vianmääritysporttiin.

Siirrettäviä tallenusvälineitä, esimerkiksi USB-muisteja voidaan usein käyttää myös ajoneuvoissa. Näiden tallennusvälineiden avulla ajoneuvoon voidaan siirtää esimerkiksi mediatiedostoja, kuten musiikkia, mutta ajoneuvoihin voidaan myös esimerkiksi asentaa päivityksiä näiden avulla. Näitä siirrettäviä tallennusvälineitä on myös mahdollista tartuttaa haittaohjelmilla, jotka voivat levitä ajoneuvon sulautettuihin järjestelmiin, kun muistin laittaa ajoneuvoon kiinni (Zhang, Antunes ja Aggarwal 2014, s. 13). Checkoway ym. (2011) löysivät tutkimuksessaan kaksi siirrettäviä tallenusvälinetä käyttävää haavoittuvuutta. Ensimmäinen haavoittuvuus liittyi järjestelmän päivittämiseen, jossa mediasoitin tunnisti tietyllä tavalla nimetyn tiedoston asetetusta muistista ja automaattisesti uudelleenasenti järjestelmän ohjelmiston asetetusta muistista löytyvällä versiolla, jos käyttäjä ei reagoinut soittimen näyttämään viestiin. Toinen haavoittuvuus perustui äänitiedoston muokkaamiseen sillä tavalla, että tiedostoon ohjelmoitiin haittaohjelma, joka lähettää ajoneuvossa paketteja CAN-väylään, eli ajoneuvon automaatiota ohjaavaan väylään (*engl. Controller area network*). Kuten ajoneuvon sisäisen vianmääritysjärjestelmän käyttö, myös siirrettävien tallenusvälineiden käyttö hyökkäykseen vaatii fyysisen pääsyn ajoneuvoon, joten riski on pieni, jos ajoneuvon käyttä-

jää ei manipuloida asentamaan haittaohjelma tallennusvälineelle itse. Käyttäjän manipuloinnista kerrotaan tarkemmin luvussa 3.4.

Itseohjautuvien ajoneuvojen ohjelmistoja on hyvä päivittää uusien ominaisuuksien ja korjausten takia. Järjestelmäpäivitykset voivat tapahtua langattomasti verkosta (*OTA, Over-the-air*) tai ulkoisen muistin avulla, kuten aiemmin mainittiin. Langattomasti päivittäminen kuitenkin altistaa päivitettävät järjestelmät mm. haittaohjelmille ulkopuolisilta sivustoilta (Zhang, Antunes ja Aggarwal 2014, s. 13). Langattomien päivitysten käyttäminen saattaa mahdollistaa järjestelmiin pääsyn myös käyttäjän manipuloinnin avulla, esimerkiksi väärennetyillä päivityksillä (*engl. Rogue updates*), joissa ajoneuvon tietokone päivittyy ohjelmistolla, joka ei ole ajoneuvon valmistajan virallisesti jakama päivitys ja saattaa sisältää piilotettuja haavoittuvuuksia (Parkinson ym. 2017, s. 2908).

Ajoneuvoihin on aloitettu myös sisällyttämään sulautettuja verkkoselaimia (*engl. Embedded Web Browsers*), joiden avulla käyttäjä voi selata internettiä, sekä ladata mediaa ja sovelluksia niin ajoneuvovalmistajalta, kuin muilta osapuolilta. Zhangin, Antunesin ja Aggarwalin (2014, s. 13) mukaan yhteys internettiin ja mahdollisuus ladata sovelluksia avaa uuden kanavan myös haittaohjelmien lataamiseen, kuten tavallisissa tietokoneissa ja älypuhelimissa. Myös jälkiasennetut laitteistot, kuten mediasoittimet, voivat aiheuttaa uhkia sulautettujen verkkoselaimien avulla saatavien kolmanten osapuolien sovelluksien takia. Nämä jälkiasennetut laitteet ovat useasti Linux-, Windows- tai Android-pohjaisia järjestelmiä ja ne ovat helposti muokattavissa suorittamaan haitallisia sovelluksia (Zhang, Antunes ja Aggarwal 2014, s. 13). Myös näiden laitteiden yleinen tietoturvataso voi olla kyseenalainen vähäisten päivitysten tai päivittämättömyyden takia, koska itse ajoneuvon käyttäjä jää vastuuseen niiden päivittämisestä ja kyberturvallisuudesta niiden ollessa jälkiasennettuja.

## 3.3 Verkkohyökkäykset

Verkkohyökkäyksiä ajoneuvoihin voi tapahtua monella eri teknologialla. Itseohjautuvissa ajoneuvoissa on monia lyhyen ja pitkän kantaman verkkoteknologioita, joita on mahdollista hyödyntää hyökkäyksissä.

Lyhyen etäisyyden hyökkäykset käyttävät nimensä mukaisesti verkkoja, jotka ovat tarkoi-

tettu lyhyen etäisyyden kommunikointiin infrastruktuurin, muiden ajoneuvojen ja laitteiden kanssa. Parkinsonin ym. (2017, s. 2909) mukaan monessa nykyajoneuvossa on sisäänrakennettu Bluetooth-valmius median siirtämistä varten. Tämä saattaa aiheuttaa haavoittuvuuden ajoneuvoon esimerkiksi aiemmin mainitun Checkowayn ym. (2011) tutkimuksen kaltaisissa tapauksissa, joissa mediatiedoston kautta päästiin käsiksi ajoneuvon automaatiota ohjaavaan väylään. Haataja (2009) osoittaa kirjassaan myös monia bluetooth-laitteiden haavoittuvuuksia ja korostaa miten huonolla pohjalla bluetooth-laitteiden kyberturvallisuus on. Hänen mukaan esimerkikiksi salaus ei ole bluetooth-laitteiden vakioasetuksissa päällä. Itseohjautuvissa ajoneuvoissa bluetooth voi näiden haavoittuvuuksien takia olla yksi pahimmista potentiaalisista hyökkäyskanavista, varsinkin verrattaessa muihin lähietäisyyden haavoittuvuuksiin.

Avaimeton käynnistys ja keskuslukitusjärjestelmä on Parkinsonin ym. (2017, s. 2909) mukaan ollut helppo kohde kaapata avaimen signaali alkeellisissa järjestelmissä. Heidän mukaansa kuitenkin myös moderneissa ja arvokkaissa ajoneuvoissa on havaittu haavoittuvuuksia liittyen näihin teknologioihin. Tälläinen haavoittuvuus ei sinäänsä ole ajoneuvon käyttäjän turvallisuudelle riski, mutta altistaa ajoneuvon sen varastamiselle näiden teknologioiden kautta. Tällainen haavoittuvuus mahdollistaa myös esimerkiksi etälaitteen asentamisen OBD-porttiin tai ajoneuvon saastuttamisen fyysisellä muistilla ajoneuvon omistajan ollessa muualla.

Itseohjautuvat ajoneuvot keskustelevat myös infrastruktuurin ja muiden ajoneuvojen kanssa langattomasti. Näiden langattomien signaalin häirintä (*engl. Signal jamming*) on Parkinsonin ym. (2017, s. 2910) mukaan edullinen ja hyvin saatavilla oleva tapa vaikuttaa itseohjautuvan ajoneuvon toimintaan. Signaalin häirintä voi heidän mukaansa aiheuttaa turvallisuusriskejä ajoneuvon käyttäjälle, koska ajoneuvo voi häirinnän seurauksena menettää infrastruktuurilta ja muilta ajoneuvoilta saatavaa tärkeää tietoa. Signaalin häirintää voi Parkinsonin ym. (2017, s. 2910) mukaan tapahtua myös ajoneuvossa olevien langattomien sensoreiden ja ajoneuvon välillä, esimerkiksi renkaiden paineenvalvontajärjestelmissä, kuten aikaisemmin on mainittu.

Ajoneuvot kommunikoivat ulkomaailman kanssa myös pitkän etäisyyden verkossa esimerkiksi langattoman lähiverkon tai matkapuhelinverkon kautta. Parkinsonin ym. (2017, s. 2910) mukaan tämä aiheuttaa mahdollisuuksia haavoittuvuuksia laitteistossa, jotka voivat esimerkiksi antaa etäyhteyden ajoneuvon automaatiota ohjaavaan väylään. Heidän mukaansa yh-

teysmahdollisuus kuitenkin toisaalta mahdollistaa esimerkiksi hätäjärjestelmien toiminnan, esimerkiksi sensoreilta saatu data törmäyksestä voi laukaista suoraan hätäpuhelun.

Yhteys internettiin mahdollistaa myös muita erilaisia ajoneuvoon kohdistuvia verkkohyökkäyksiä. Näitä hyökkäystyyppejä ovat Parkinsonin ym. (2017, s. 2910) mukaan esimerkiksi:

1. Salasana- ja avainhyökkäykset: Hyökkäyksiä, jossa järjestelmään pääsyyä rajoittavia mekanismeja testataan jatkuvasti kokeilemalla erilaisia salasanoja tai avaimia, kunnes pääsy saadaan.
2. Palvelunestohyökkäykset (*engl. DDoS, Distributed Denial of service*): Hyökkäyksiä, joissa normaali järjestelmän toiminta ruuhkautetaan käyttäen yhtä tai useampaa hyökkäävää tietokonetta. Tämän tyyppiset hyökkäykset voivat vaikuttaa ajoneuvoissa liikenteen ruuhkautumiseen ja jopa aiheuttaa törmäyksiä, koska törmäystä estävät mekanismit eivät saa dataa tarpeeksi ajoissa tai ollenkaan.
3. Verkkoprotokollahyökkäykset: Hyökkäyksiä, joissa verkkoprotokollien toimintaa tutkitaan mahdollisten haavoittuvuuksien löytämiseksi. Löytämisen jälkeen hyökkääjä voi käyttää löytynyttä haavoittuvuutta ajoneuvoon hyökkäämiseen.

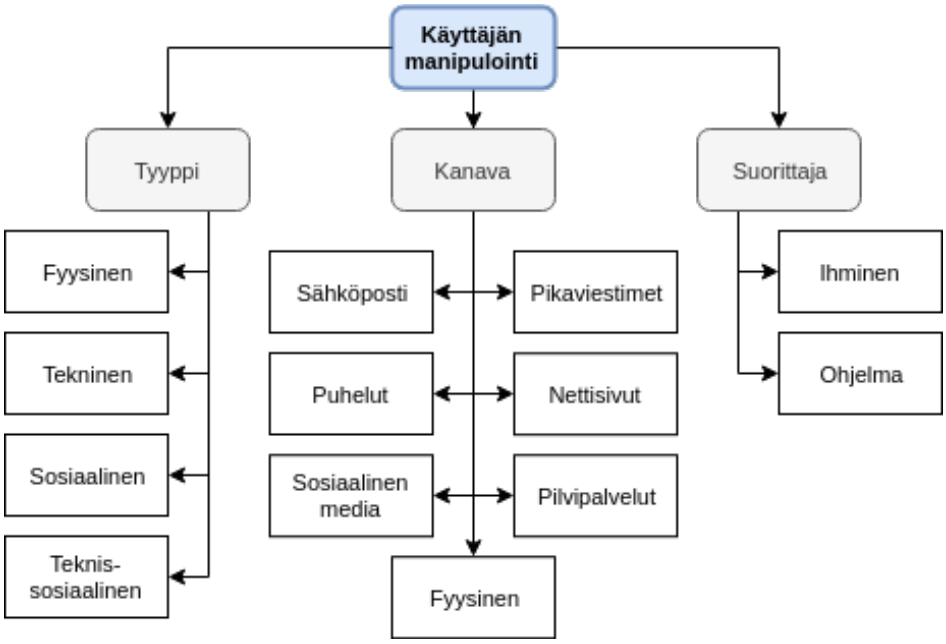
Yksi pitkän etäisyyden yhteystapa internetin lisäksi on radiojärjestelmät. Näihin järjestelmiin kuuluu Parkinsonin ym. (2017, s. 2911) mukaan jo aiemmin mainitun maailmanlaajuisen paikallistamisjärjestelmän lisäksi digitaaliradio, radion datajärjestelmä (*engl. RDS, Radio Data System*) ja liikenneviestijärjestelmät. Hänen mukaansa on todennäköistä, että nämä järjestelmät ovat osa ajoneuvon automaatiota ohjaavaa väylää. Tämän takia myös haavoittuvuudet näissä järjestelmissä voivat olla kyberturvallisuusriski.

## 3.4 Käyttäjän manipulointi

Käyttäjän manipulointi (*engl. Social engineering*) on tapa saada käyttäjä altistamaan käyttämänsä tietojärjestelmä hyökkäyksille käyttäen hyväkseen hyökkääjän vaikutusvaltaa, luottamusta, suostuttelua ja käyttäjän tiedottomuutta. Tekniset suojaukset ovat yleensä tehottomia tälläisiä hyökkäyksiä vastaan (Krombholz ym. 2015, s. 114).

Tietojärjestelmiä käyttävät ihmiset ovat yleensä jollain tasolla perehtyneitä käyttämäänsä

teknologiaan, mutta ajoneuvoja käyttävät ihmiset, joilla ei välttämättä ole suurta kokemusta tietojärjestelmistä ja käytössä olevista teknologioista. Ajoneuvojen käyttäjien potentiaali toimia kyberturvallisuusriskinä on tämän takia suurempi. Kokematon käyttäjä saattaa aiheuttaa potentiaalisen kyberturvallisuusriskin olemalla niin sanotusti helppo saalis hyökkääjälle ja antamalla tahtomattaan hyökkääjälle helpon pääsyn ajoneuvon tietojärjestelmiin esimerkiksi lankeamalla tietojenkalasteluyrityksiin (Parkinson ym. 2017, s. 2905).




Kuvio 2. Käyttäjän manipuloinnin tyypit, kanavat ja suorittajat Krombholzin ym. (2015, s. 115-116) mukaan.

Kuten kuviossa 2 nähdään, käyttäjän manipulointi voidaan jakaa neljään eri tyyppiin: fyysiseen, tekniseen, sosiaaliseen ja teknis-sosiaaliseen. Erilaiset hyökkäystavat hyödyntävät näistä yhtä tai useampaa eri muotoa hyökkäykselle. Hyökkäyksissä voi myös yhdistyä useampi eri kuviossa 2 näkyvä kanava sekä suorittaja. Pääasiallisia hyökkäystapoja on Krombholzin ym. (2015, s. 117) mukaan mukaansa seitsemän erilaista:

1. Kalastelu (*engl. Phishing*): yritys saada haltuun arkaluontoista tietoa esiintymällä luotettavana tahona. Kalasteluyritykset kohdistetaan yleensä suurille massoille ihmisiä. Kohdistettu kalastelu (*engl. spear-phishing*) kohdistuu yksittäiseen henkilöön tai yritykseen, mutta vaatii hyökkääjältä paljon enemmän esitietoa kohteesta.

2. Dyykkays (*engl. Dumpster diving*): tapa kerätä tietoa kohteesta käymällä läpi sen pois heittämiä roskia ja tavaroita, joissa saattaa olla arkaluontoista tietoa tai tietoa jolla voidaan päästä käsiksi kohteen järjestelmään tai käyttäjätunnukseen.
3. Kurkkiminen (*engl. Shoulder surfing*): tapa saada haltuun tietoa tarkkailemalla kohdetta, esimerkiksi jonkun näppäimistön tai näytön kurkkiminen "olan yli".
4. Käänteinen käyttäjän manipulointi (*engl. Reverse social engineering*): hyökkäystapa, jossa hyökkääjä yrittää saada kohteen luottamuksen esimerkiksi luomalla keinotekoisen ongelmatilanteen, jossa kohde tarvitsee apua ja auttamalla uhria tässä tilanteessa.
5. Houkutussivustot (*engl. Waterholing*): tapa saada haltuun kohteen tietoja murtautumalla kohteen yleisesti käyttämään sivustoon tai sovellukseen ja keräämällä kohteen tietoja sen kautta, kun kohde käyttää sitä.
6. Jatkuva uhka (*engl. Advanced Persistent Threat*): tarkoittaa pitkäaikaista, yleensä internetpohjaista kohteen vakoilua ilman, että kohde saa tietää tästä. Esimerkiksi kohteen tietokoneeseen asennettu tietoja keräävä haittaohjelma.
7. Houkuttelu (*engl. Baiting*): hyökkäystapa, jossa saastutettu tallennusväline jätetään paikkaan, josta kohde voi sen löytää.

Suurin osa näistä hyökkäyksistä ei vaikuta suoraan ajoneuvon kyberturvallisuuteen, mutta näitä tapoja voidaan käyttää esimerkiksi käyttäjän salasanan saamiseksi, jonka avulla hyökkääjä voi päästä myös ajoneuvoon käsiksi. Koska näiltä haavoittuvuuksilta suojautuminen teknisesti on todella vaikeaa, tulisi käyttäjän tietämyksen parantamiseen käyttää aikaa. Ilman oikenlaista tietämystä näistä haavoittuvuuksista ei käyttäjä pysty millään tavalla itse näiltä suojautumaan aiheuttaen näin omalle ja muiden turvallisuudelle suuren riskin.

# 4 Yhteenveto

Itseohjautuvissa ajoneuvoissa on paljon mahdollisia kyberturvahaavoittuvuuksia. Erilaisia häirintäkeinoja voidaan käyttää ajoneuvon datan väärentämiseksi ja murtautumiskeinoja voidaan käyttää ajoneuvon hallinnan saamiseksi. Haavoittuvuuksia on monessa eri teknologiassa, joten suojautuminen näitä haavoittuvuuksia vastaan vaatii monen eri teknologian kehittämistä turvallisempaan suuntaan. Kyberturvallinen ajoneuvo muodostuu vasta, kun kaikki ajoneuvossa käytettävät teknologiat on suojattu tarpeeksi hyvin, sillä yksittäisen teknologian haavoittuvuus voi jo aiheuttaa ajoneuvossa suuren riskin ja esimerkiksi antaa pääsyn muihin järjestelmiin.

Ajoneuvon sisäisiä teknologioita, kuten sensoreita voidaan usein häiritä todella helposti ja edullisesti. Koska nämä sisäiset järjestelmät tuottavat tärkeän osan datasta, johon ajoneuvon toiminta perustuu, tulisi näiden häirtsemistä pyrkiä estämään jollain tavalla. Näiden teknologioiden dataa pitäisi myös pystyä vertailemaan ja tutkimaan reaaliajassa, jotta virheellinen ja väärä data voitaisiin tunnistaa ja suodattaa pois.

Yhteys muihin laitteisiin tuo itseohjautuville ajoneuvoille paljon ominaisuuksia, joista on hyötyä, mutta ne tuovat myös riskinä ajoneuvoihin mahdolliset haittaohjelmat. Haittaohjelmia on mahdollista asentaa ajoneuvoihin monien eri teknologioiden kautta. Nämä teknologiat saattavat mahdollistaa haittaohjelmalle täyden pääsyn ajoneuvon järjestelmiin, joten suojautuminen haittaohjelmia vastaan tulisi toteuttaa viimeistään tällaisen teknologian ja ajoneuvon muiden teknologioiden ja ohjausjärjestelmien välisissä rajapinnoissa. Myös näiden yksittäisten teknologioiden suojausta tulisi yleisesti parantaa, esimerkkinä Bluetooth, jonka suojaus on todella huono jo itsessään (Haataja 2009).

Käyttäjän manipulointi on merkittävä haavoittuvuus kaikissa tietojärjestelmissä, koska teknologista suojausta on todella vaikea näille hyökkäyksille toteuttaa (Krombholz ym. 2015). Koska itseohjautuvat ajoneuvot ovat myös tietojärjestelmiä, myös käyttäjän manipulointi pätee niihin. Käyttäjän manipuloinnin teknisen helppouden ja sen aiheuttamien riskien takia tämä haavoittuvuus on yksi tärkeimmistä osa-alueista itseohjautuvien ajoneuvojen kyberturvallisuutta kehitettäessä. Suojautuminen käyttäjän manipuloinnin vaikutukselta vaatiikin

käyttäjän kouluttamista ja tietoisuuden lisäämistä näiden hyökkäyksien toimintatavoista ja riskeistä.

# Lähteet


Checkoway, Stephen, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner ja Tadayoshi Kohno. 2011. "Comprehensive Experimental Analyses of Automotive Attack Surfaces". *USENIX Security Symposium* 4:447–462.

Committee, SAE On-Road Automated Vehicle Standards, ym. 2014. "Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems". *SAE Standard J* 3016:1–16.

Haataja, Keijo. 2009. *Security Threats and Countermeasures in Bluetooth-Enabled Systems.* University of Kuopio. ISBN: 978-951-27-0111-7.

Jeske, Tobias. 2013. *Floating Car Data from Smartphones: What Google and Waze Know about You and How Hackers Can Control Traffic.*

Krombholz, Katharina, Heidelinde Hobel, Markus Huber ja Edgar Weippl. 2015. "Advanced Social Engineering Attacks". *Journal of Information Security and Applications* 22 (kesäkuu): 113–122. ISSN: 22142126. doi:10.1016/j.jisa.2014.09.005.

Parkinson, Simon, Paul Ward, Kyle Wilson ja Jonathan Miller. 2017. "Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges". *IEEE Transactions on Intelligent Transportation Systems* 18, numero 11 (marraskuu): 2898–2915. ISSN: 1524-9050, 1558-0016. doi:10.1109/TITS.2017.2665968.

Petit, Jonathan, ja Steven E. Shladover. 2014. "Potential Cyberattacks on Automated Vehicles". *IEEE Transactions on Intelligent Transportation Systems:* 1–11. ISSN: 1524-9050, 1558-0016. doi:10.1109/TITS.2014.2342271.

Zhang, Tao, Helder Antunes ja Siddhartha Aggarwal. 2014. "Defending Connected Vehicles Against Malware: Challenges and a Solution Framework". *IEEE Internet of Things Journal* 1, numero 1 (helmikuu): 10–21. ISSN: 2327-4662. doi:10.1109/JIOT.2014.2302386.