Joonas Rautiainen

Henkilöautojen kyberturvallisuus

Tietotekniikan kandidaattitutkielma

25. toukokuuta 2021

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Joonas Rautiainen

Yhteystiedot: jopevira@student.jyu.fi

Ohjaaja: Timo Tiihonen

Työn nimi: Henkilöautojen kyberturvallisuus

Title in English: Cybersecurity of passenger cars

Työ: Kandidaattitutkielma

Sivumäärä: 20+0

Tiivistelmä: Henkilöautojen kyberturvallisuus on ajankohtainen aihe, joka tulee nousemaan pian selkeämmin esille. Kyberturvallisuus on otettava paremmin huomioon kaikkien ajoneuvojen kehityksessä. Tutkielmassa havaitaan lisääntyvät teknologian tuomia ongelmia. Huomataan, että henkilöautoihin kohdistuvat kyberhyökkäykset eivät vielä ole suuri ongelma, mutta jos kyberturvallisuuteen ei aleta kiinnittää paremmin huomiota, voi tulevaisuudessa olla ongelmia odotettavissa. Henkilöautojen kyberturvallisuus tulee ottaa vakavasti ennen kuin on myöhäistä.

Avainsanat: kyberturvallisuus, autot, ohjelmistot, ECU, CAN, kyberhyökkäys

Abstract: Cyber safety in passenger cars is an issue that will soon come to the up more clearly. Cybersecurity needs to be better considered in the development of all vehicles. The dissertation observes increasing problems brought about by technology. It is noted that cyberattacks on passenger cars are not yet a major problem, but if better attention is not paid to cybersecurity, problems may be expected in the future. Cybersecurity of passenger cars must be taken seriously before it's too late.

Keywords: Cybersecurity, cars, softwares, ECU, CAN, cyber attack

Kuviot

Sisällys

1 Johdanto

Nykyaikaisista ajoneuvoista löytyy paljon erilaisia käyttäjien elämää helpottavia teknologioita. Tänä päivänä puhutaan yhdistetyistä autoista, jotka pystyvät kommunikoimaan sekä älylaitteiden kanssa, että muiden liikenteessä olevien ajoneuvojen ja infrastruktuurin kanssa. Näillä pyritään vähentämään kuljettajan taakkaa ajaessa sekä lisäämään turvallisuutta. Ajoneuvoissa on koko ajan enemmän mahdollisuuksia uusien laitteistojen ja ohjelmistojen myötä (Coppola ja Morisio 2016). Nykyaikaset henkilöautot ovat yhteydessä internetiin monien eri teknologioiden kautta ja näihin yhteyksiin sisältyy monia riskejä tietoturvallisuuden näkökulmasta. On odotettavaa, että kyberhyökkäysten määrä henkilöautoja kohtaan tulee kasvamaan lähitulevaisuudessa.

Tämä on pienimuotoinen kirjallisuuskatsaus, joka syventyy nykyaikaisten henkilöautojen sisältämään tekniikkaan ja ohjelmistoihin sekä niistä syntyviin turvallisuus riskeihin. Erityisesti syvennytään eri teknologioista johtuviin ongelmiin, mutta myös ohjelmistojen ongelmista yleisellä tasolla. Katsaus painottuu henkilöautoihin, jotka ovat yhteydessä ulkomaailmaan.

Luvussa 2 perehdytään henkilöautojen sisältämiin ohjelmistoihin sekä käydään vähän läpi niihin liittyviä riskejä. Lisäksi listataan erilaisia haittaohjelmia, joita voitaisiin käyttää autoja kohtaan. Kolmas luku painottuu teknologioihin, joiden kautta mahdolliset haittaohjelmat voitaisiin saada henkilöautoihin. Samalla käydään hieman läpi eri teknologioiden sisältämiä riskejä ja heikkouksia. Neljännessä luvussa puolestaan käydään pintapuolisesti läpi konkreettisia esimerkkejä hyökkäyksistä, joita henkilöautoihin on kohdistunut. Lopussa vielä esitellään muutama tapa, joita on ehdotettu autojen kyberturvallisuuden parantamiseksi.

2 Ohjelmistot nykyaikaisissa henkilöautoissa

Henkilöautot sisältävät nykyään valtavan määrän tietotekniikka. Coppola ja Morisio (2016) kertovat kuinka ensimmäiset ohjelmistokomponentit on lisätty autoihin yli kolmekymmentä vuotta sitten. Tällä hetkellä autoista löytyy jopa yli 100 miljoona riviä koodia ja määrä on suuressa kasvussa. Nykyaikaiset autot sisältävät siis valtavat määrät erilaisia ohjelmistoja (Levi, Allouche ja Kontorovich 2018).

Jopa halvemmista perustason henkilöautoista löytyy kymmeniä moottorinohjausyksiköitä eli ECU:ja (eng. Engine Control Unit). Niitä on ympäri autoa ovissa, rungossa, istuimissa ja kaikkialla minne autojen suunnittelijat ovat keksineet niitä laittaa (Charette 2009). Charetten mukaan nykyaikaisten autojen hinnasta jopa 35–40 prosenttia tulee ohjelmistoista ja elektroniikasta. Ohjelmistojen määrä tuo väistämättä ongelman, jossa mahdollisilla hakkereilla on koko ajan enemmän uusia ohjelmistoja, joista etsiä haavoittuvuuksia.

Henkilöautojen ohjelmistojen kehityksessä on ollut nähtävillä melko yleinen ilmiö. Kehitys on ollut niin nopeaa, että ohjelmistoja on kiirehditty valmiiksi ja niiden turvallisuus on saattanut jäädä osittain vajaaksi (Bécsi, Aradi ja Gáspár 2015).

Bécsi, Aradi ja Gáspár (2015) kertovat kuinka koko yhdistettyjen autojen konsepti on heterogeeninen ja monipuolinen. Siinä kehitetään useita eri standardeja, eikä käytössä ole parhaiksi todettuja käytäntöjä. Kehitys autoteollisuudessa viittaa siihen, että uusia yhdistämisen ratkaisuja otetaan käyttöön vaihe vaiheelta ja esimerkiksi turvallisuudelle epäkriittisiä järjestelmiä vaihdetaan nopeasti monimutkaisempiin järjestelmiin.

2.1 Käyttäjän hallinnassa olevat toiminnot

Nykyaikaiset henkilöautot ovat käytännössä tietokoneita, joten ne myös sisältävät käyttöjärjestelmän, jonka avulla ohjelmistoja voidaan käyttää. Monet suuret ohjelmistoyritykset ovat lähteneet mukaan käyttöjärjestelmien kehittämiseen. Newcomb (2012) kertoo kirjoittamassaan artikkelissa, kuinka esimerkiksi Microsoft, sekä Android on ollut mukana tekemässä käyttöliittymiä ajoneuvoihin. Yksi suosituimmista on QNX, joka on Unix pohjainen monen

suuren autovalmistajan käyttämä käyttöliittymä.

Zhang, Antunes ja Aggarwal (2014) toteavat, että Linux pohjaiset käyttöliittymät ovat myös suosittuja Linuxin hyvän virusturvan takia. BMW:n kumppaneidensa kanssa aloittama GENIVI onkin suosittu monien suurien autovalmistajien keskuudessa. Linux pohjaisena ratkaisuna löytyy myös Intelin tukema Tizen IVI sekä avoimeen lähdekoodiin perustuva Automotive Grade Linux, joka on tehty Tizen IVI:n pohjalta (Coppola ja Morisio 2016).

Näiden käyttöliittymien kautta auton kuljettajalla voi olla pääsy moniin eri toimintoihin. Musiikin soittamisella ei vielä vaaratilanteita saada aikaiseksi, mutta esimerkiksi jousituksen säätämäinen kesken ajon voi olla jo huomattavasti vaarallisempaa. Näihin toimintoihin käsiksi päästäessä voidaan siis aiheuttaa hyvinkin suurta harmia.

2.2 Ajoneuvojen käyttämät ekosysteemipalvelut

Useilta autovalmistajilta löytyy järjestelmät, joiden kautta autot kommunikoivat esimerkiksi valmistajan palveluiden kanssa. Onishin (2012) mukaan suurella osalla autovalmistajista on omat järjestelmät, jotka voivat toimia esimerkiksi älypuhelimen kautta. Jos hakkerit pääsevät näihin käsiksi, on heillä pääsy suureen määrään autoja, ennen kuin vuoto saadaan korjattua.

Tästä on olemassa jo valmis esimerkki. BMW:n ConnectedDrivessä käytettiin Combox-nimistä yhdyskäytävää, joka oli tarkoitettu esimerkiksi hätäpuheluiden hoitamiseen ja sillä oli täten alhaisemmat turvallisuusvaatimukset. Kuitenkin mahdollisesti kiireen takia kyseinen yhdyskäytävä oli liitetty auton sisäiseen verkkoon sekä kaukolukitukseen. Näin hakkerit saivat reitin tehdä tuhoa BMW:n ohjelmistolle (Bécsi, Aradi ja Gáspár 2015).

2.3 Kriittiset reaaliaikaiset ohjausjärjestelmät

Suurimmasta osasta auton reaaliaikaisesta toiminnasta on vastuussa ympäri autoa olevat ECU:t. Coppola ja Morisio (2016) kertovat, että ECU:jen vastuulla on paljon erilaisia erittäin kriittisiäkin toimintoja. Esimerkiksi polttoaineen syöttö, turvatyynyjärjestelmä ja jarrut toimivat ECU:jen avulla.

Jokainen auton ECU sisältää ohjelmiston ja on näin mahdollinen kohde hakkereiden toimille. Bécsin, Aradin ja Gáspárin (2015) mukaan ECU:jen ohjelmistoon käsiksi pääsemiseen on kaksi takaporttia. Ensimmäiseksi takaportiksi he kertovat nykyaikaisten ECU:jen monimutkaisuudesta johtuvat auki jääneet tunkeutumismahdollisuudet. Toiseksi mahdolliseksi takaportiksi he mainitsevat sen, että ECU:un on tarkoituksella jätetty reitti mahdollisesti vaikkapa vianmääritystä varten.

Toinen ongelma ECU:jen kanssa on se, että niiden pitää itse päätettävä mitä sille tulevilla komennoilla tehdään. Näin esimerkiksi todennusta huijaamalla, voidaan ECU:un saada lähetettyä muutettuja ohjelmistoja ja näin saadaan avattua mahdollisuuksia hyökkäyksille. (Bécsi, Aradi ja Gáspár 2015)

2.4 Hyökkäykset ohjelmistoihin

Mahdollisia haittaohjelmia löytyy useampia erilaisia. Koska autot ovat nykyään käytännössä tietokoneita, ei mitään näistä tyypillisistä haittaohjelmista voi unohtaa autojen suunnittelussa. Näitä ovat Zhangin, Antunesin ja Aggarwalin (2014) mukaan

1. Virus on haittaohjelma, joka osaa lisääntyä ohjelmasta ja tiedostosta toiseen. Se pyrkii leviämään koko ajan laajemmalle. Tämä voisi käytännössä autossa esimerkiksi tarkoittaa koko autoa ja tätä kautta valmistajan palveluihin.
2. Mato on haittaohjelma, joka leviää tietokoneelta toiseen tarvitsematta kiinnittyä itse ohjelmiin.
3. Troijalainen on haittaohjelma, joka näyttäisi tekevän asiaa mitä siltä on alun perin haluttu, mutta samalla se saa luvattoman pääsyn tietokoneeseen. Tallainen voisi levitä helposti autoon esimerkiksi omistajan asentaman päivityksen tai muun vastaavan mukana.
4. Spyware eli Vakoiluohjelma on ohjelma, joka vakoilee tietokonetta ja lähettää sen tietoja muille tahoille omistajan tietämättä asiasta. Tallainen voisi helposti kerätä tietoja autosta esimerkiksi omistajan puhelimessa.
5. Ransomware eli kiristysohjelma on nimensä mukaisesti ohjelma, joka rajoittaa tartunnan saanutta tietokonetta ja vaatii lunnaita omistajalta. Bajpai, Enbody ja Cheng

(2020) mukaan internetin yleistyminen autoissa tuo kiristysohjelmille mahdollisuuksia myös autoja kohtaan.

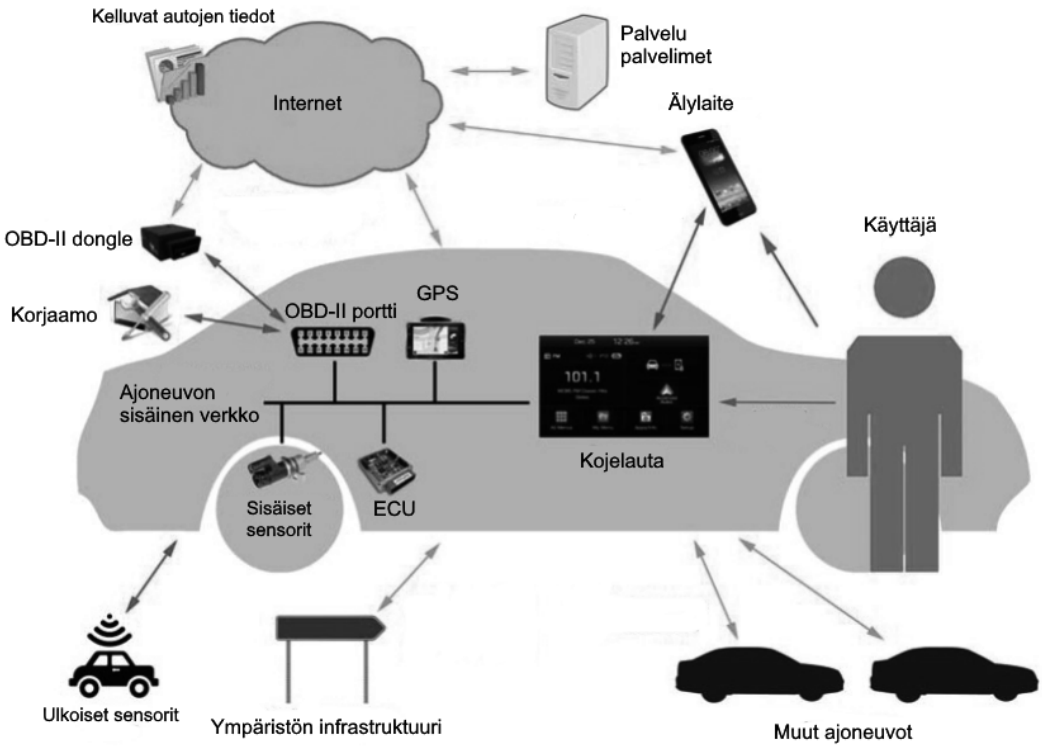
6. Rootkit on ohjelmisto, jonka tarkoitus on piilottaa edellä mainittujen haittaohjelmien poissaolo. Sen asentaminen vaatii tietokoneen täydet oikeudet, mutta myös sen poistaminen on erityisen hankalaa.

Tämän lisäksi haittaohjelmat on vielä jaettu kahteen osaan. Niin sanotut polymorfiset haittaohjelmat, joiden koodirunko pysyy aina samana, mutta salaus muuttuu joka kerta. Metamorfiset haittaohjelmat taas osaavat muokkautua kokonaan niin, että sillä ei ole mitään samana pysyvää vakio osaa (Zhang, Antunes ja Aggarwal 2014).

Näiden haittaohjelmien pääsy ajoneuvon tietokoneisiin ei vielä itsessään riitä vahingoittamaan järjestelmiä, vaan niiden täytyy onnistua lisäksi löytämään heikkouksia. Kuitenkin autojen ollessa käytännössä tietokoneita, on erittäin tärkeää ottaa ohjelmistojen kehityksessä huomioon kaikki mahdolliset haittaohjelmat. Jokainen edellä mainituista haittaohjelmistoista voi olla henkilöautossa vaarallinen tai vähintään haittaa aiheuttava.

3 Henkilöautojen kommunikointiteknologiat

Henkilöautot sisältävät nykyään monia eri teknologioita, joiden avulla auto kommunikoi sekä omien eri yksiköidensä välillä, että auton ulkopuolisen maailman kanssa. Ajoneuvojen ohjelmistoihin voidaan saada yhteys montaa eri kautta.



Kuvio 1. Kuva henkilöauton kommunikaatioteknologioista Coppola ja Morisio (2016) mukaan.

3.1 Henkilöautojen sisäinen kommunikointi

Henkilöautot sisältävät noin 70–100 elektronista ohjausyksikköä eli ECU:a, jotka huolehtivat käytännössä kaikesta autojen sähköisestä toiminnasta (Levi, Allouche ja Kontorovich 2018). Näiden välinen yhteydenpito tapahtuu yleensä CAN-väylän avulla. CAN-väylä on automaatioväylä (eng. control area network), joka lähettää aina kaikki käskyt kaikille verkossa oleville laitteille ja viestejä vastaanottava ECU päättää onko kyseinen viesti tarkoitettu

sille (Levi, Allouche ja Kontorovich 2018).

CAN-väylän suojaamattomuus ja sen pääsy esimerkiksi turvatyynyjen ja jarrujen ohjauksesta huolehtiviin yksiköihin tekee siitä halutun hakkereiden näkökulmasta. CAN-väylällä ei ole digitaalista allekirjoitusta eikä sitä ole suojattu millään protokollalla, joka varmistaisi informaation turvallisuuden (Coppola ja Morisio 2016). ECU:t ovat uudelleen ohjelmoitavissa ja niiden kautta pystyttäisiin aiheuttamaan mahdollisesti suuriakin haittoja. Onkin siis oleellista käydä läpi, mitä ovat nämä mahdolliset reitit CAN-väylään ja sitä kautta ECU:hin on.

3.2 Fyysiset portit auton sisäiseen verkkoon

Suorin reitti auton sisäiseen verkkoon ovat fyysiset portit, joita henkilöautoissa on nykyään useita. Niiden käyttämisessä ei tarvitse kiertää hankalia langattomien yhteyksien protokollia, joten niiden käyttäminen on sen osalta helpompaa. Niiden hankaluus hakkereiden näkökulmasta tuleekin esille siinä, että haittaohjelman sisältämä laite pitää päästä kytkemään autoon fyysisesti. Yleisin tapa todennäköisesti onkin pyrkiä saamaan haittaohjelma käyttäjän laitteeseen, jonka käyttäjä itse yhdistää autoonsa.

Nykyaikaisissa moderneissa autoissa on hyvin usein jonkinlainen USB-liitäntä. Tämän liitännän avulla voidaan esimerkiksi päivittää auton tietokoneita tai suoratoistaa musiikkia auton kaiuttimista. USB-laitteeseen on helppoa saada upotettua haittaohjelmia, jotka näyttävät samalta kuin halutut ohjelmat.

Toinen erittäin yleinen fyysinen portti, joka löytyy käytännössä kaikista 2000-luvun henkilöautoista, on OBD-portti eli sisäinen diagnostiikkaportti (eng. Onboard Diagnostic). Sen kautta autosta saa paljon tietoa ja siitä on suora pääsy auton CAN-väylään ja ECU:hin (Zhang, Antunes ja Aggarwal 2014). Sitä käytetään esimerkiksi ajoneuvojen vikakoodien lukuun ja huollon yhteydessä haluttujen tietojen nollaamiseen. Sen haasteeksi muodostuukin sama ongelma, kuin USB-portilla, eli se tarvitsee jonkin laitteen fyysisesti liitettäväksi OBD-porttiin. Toisaalta se on myös suoraviivaisin reitti suoraan ECU-yksikköjen ohjelmointiin ja myös yleensä nimenomaan siihen tarkoitettukin.

OBD-II donglet ovat laitteita, joilla käyttäjä jaa itse luettua esimerkiksi autonsa vikakoodit. Donglet yhdistetään yleensä puhelimeen tai tietokoneeseen USB:n avulla. (Coppola ja Morisio 2016). Näissä laitteissa on kuitenkin myös turvallisuus riski. Dongle voidaan esimerkiksi jättää autoon paikoilleen, jolloin autoon on taas uusi mahdollinen reitti päästä käsiksi, vieläpä suoraan CAN-verkkoon. Myös itse dongleen on mahdollista saada upotettua haittaohjelmia.

3.3 Langattomat yhteydet henkilöauton ja ulkomaailman välillä

Lähes kaikista moderneista henkilöautoista löytyy jonkinlainen langaton yhteys ulkomaailmaan. Auto voi olla suoraan yhteydessä valmistajan palveluihin esimerkiksi GSM-yhteyden avulla. Toinen mahdollinen tapa yhdistää auto ulkomaailmaan ja sitä kautta valmistajan palveluihin on omistajan puhelimen kautta. Tällöin puhelin yhdistetään ensin ajoneuvoon ja sitten jonkin palvelun kautta valmistajaan. Tähän yleisimmin käytettyjä teknologioita ovat Bluetooh, WiFi ja NFC (Bécsi, Aradi ja Gáspár 2015).

Älylaitteiden yhdistämistä autoihin käytetään tukemaan turvallisuutta esimerkiksi handsfree-puheluiden avulla, tai laitteiden sovellusten käyttöön, kuten esimerkiksi musiikin toistamiseen ajoneuvon äänentoiston kautta (Zhang, Antunes ja Aggarwal 2014). Onishi (2012) kertoo, että älylaitteilla on suuret mahdollisuudet saada tartunta, sillä niillä on monia eri käyttötarkoituksia ja niitä on voitu käyttää monissa eri verkoissa. Tässä kohtaa mukaan tulee myös käyttäjän vastuu. Internet on täynnä erilaisia haittaohjelmia ja on odotettavaa, että tätä pyritään käyttämään hyödyksi myös ajoneuvoihin kohdistuvissa hyökkäyksissä.

Toinen suuri riski on mahdollisten hyökkäysten kohdistaminen itse teknologoihin, joilla puhelin yhdistetään autoon. Coppola ja Morisio (2016) toteavat, että Wifi ja Bluetooth yhteyksiin tunkeutuminen on nykyään mahdollista, ellei jopa triviaalia. Woo, Jo ja Lee (2014) ovat onnistuneet tutkimuksessaan tunkeutumaan CAN-väylän heikkouksiin langattomien yhteyksien avulla.

Myös valmistajien käyttämät palvelut, kuten esimerkiksi pilvipalvelut voivat olla hyökkäyksen kohteena. Nämä ovat erityisen vaarallisia, sillä silloin on mahdollista päästä yhteyteen useampaan ajoneuvoon kerralla. Bécsi, Aradi ja Gáspár (2015) kertovat kuinka esimerkik-

si BMW:n ConnectedDrive järjestelemään on onnistuttu tunkeutumaan ja tätä kautta päästy käsiksi auton sisäiseen verkkoon.

Nykyään on olemassa autojen välillä olevaa kommunikointia, jossa autot jakavat keskenään informaatiota (Bécsi, Aradi ja Gáspár 2015). Tämä informaatio voi olla esimerkiksi tietoa esteistä ajoradalla tai mahdollisista liukkaista paikoista. Myös infrastruktuurin kanssa kommunikointi on nykyään mahdollista. Autot voivat kommunikoida esimerkiksi älykkäiden liikennemerkkien avulla tai ne voivat käyttää matkapuhelinverkkoa viestiäkseen autovalmistajan kanssa (Bécsi, Aradi ja Gáspár 2015).

4 Henkilöautoihin kohdistuvat hyökkäykset ja mahdollisia ratkaisuja

Haittaohjelmilla voidaan aiheuttaa monenlaisia ja monentasoisia ongelmia henkilöauton omistajalle. Riskit voidaan jakaa helposti korkeintaan harmillisiin ja potentiaalisesti vaarallisiin riskeihin. Levi, Allouche ja Kontorovich (2018) kertovat, että autojen lisääntyvä yhdistäminen lisää näitä riskejä nykyään ja tulevaisuudessa huomattavasti.

Zhang, Antunes ja Aggarwal (2014) käyvät läpi erilaisia motivaatioita hyökkäyksille. Tällaisia ovat heidän mukaansa seuraavat:

1. Hauskuus ja maine: Monet hakkerit tekevät iskujaan pelkästään näyttääkseen taitonsa. Yhdistettyjen ajoneuvojen lisääntyminen on kasvattanut kyseistä motivaatiota huomattavasti.
2. Yksityisyyden rikkominen: Autoihin hyökkäämällä voidaan saada monia henkilökohtaisia tietoja kuljettajasta ja auton liikkeistä.
3. Lunnaat: Auton toimintojen lukitseminen lunnaat mielessä.
4. Varkaus: Ehkä toistaiseksi yleisin syy hyökätä autoihin.
5. Sabotaasi: Jotkut voivat tehdä hyökkäyksiä pelkästään kiusanteko mielessä. Sabotaasilla voidaan myös pyrkiä vahingoittamaan auton valmistajan mainetta.
6. Vahingoittaa kuljettajaa tai autoa: Esimerkiksi jarruja häiritsemällä voidaan aiheuttaa jopa vaarallisia tapaturmia.
7. Liikenteen häirintä: Joskus motivaationa voi olla suuremman massan häirintä ja mahdollisesti vaikkapa suuren kaupungin liikenteen ruuhkauttaminen.

Nämä kaikki ovat sellaisia motivaatioita, joiden myötä autoihin kohdistuvat hyökkäykset tulevat todennäköisesti lisääntymään.

4.1 Haittaa aiheuttavat hyökkäykset

Henkilöautojen kohdalla voidaan ajatella harmillisiksi haittaohjelmilla aiheutetuiksi ongelmiksi esimerkiksi autoon murtautuminen. Zhangin, Antunesin ja Aggarwalin (2014) mu-

kaan Yhdysvalloissa valmistettavista autoista lähes kaikki tukevat avaimetonta ovien aukaisemista. Tämä voi esimerkiksi toimia niin, että avaimenperän oleminen lähellä aukaisee ovet. Zhang, Antunes ja Aggarwal (2014) puolestaan kertovat tapauksesta, jossa Kyseisiä järjestelmiä on onnistuttu hakkeroimaan. Heidän mukaansa tämä voi onnistua, vaikka auton omistaja olisi kaukana autosta.

Tallaisiin hyökkäyksiin tarvittavien välineiden hinta on alhainen, joten tämä lisää mahdollisten hakkeroitumisien määrää merkittävästi. Ibrahimin ym. (2018) esimerkki tukee edellisiä väitteitä. He esittelevät skenaarion, jossa halvalla Raspberry Pi pohjaisella laitteella pystytään häiritsemään yhteyksiä siten, että omistaja joutuu käyttämään fyysistä avainta. Samalla laitteella on myös onnistunut auton kaappaaminen vastaavalla tavalla. Jos etäisyydet ovat olleet kohdillaan, on kaappaus onnistuttu toteuttamaan jopa joka yrityksellä.

4.2 Hengenvaaralliset hyökkäykset

Vaarallisia ongelmia syntyy, kun haittaohjelmat vaikuttavat auton kriittisiin toimintoihin ja siten esimerkiksi jarruihin. Jo nyt on onnistuttu etänä sammuttamaan auton moottori keskelle moottoritietä. Autovalmistaja Chrysler joutui kutsumaan takaisin 1.4 miljoonaa Jeep Cherokee autoa tämän ongelman takia (Levi, Allouche ja Kontorovich 2018). Ring (2015) kertoo, että kyseessä oli harjoitus, mutta tapaus on kuitenkin selkeä esimerkki siitä, että kyseisenlainen hakkerointi on mahdollista. Voidaan vai kuvitella minkälaista tuhoa saataisiin aikaiseksi, jos yksittäisiä autoja alettaisiin pysäytellä keskelle moottoritietä tiheään tahtiin.

Moottorin pysäyttämisen lisäksi on muita tapoja aiheuttaa suoraa vaaraan autoilla liikkuville. Vaikkapa jarrujen ohjauksesta huolehtivan ECU:n ohjelmistoihin pääsevä haittaohjelma voisi olla erittäin kohtalokasta. Nie, Liu ja Du (2017) näyttävätkin kokeessaan, kuinka Teslan selaimen haavoittuvuuden kautta on päästy käsiksi auton jarruihin, tuulilasinpyyhkimiin sekä sivupeileihin. Tämä kaikki oli onnistuttu tekemään auton ollessa liikkeellä. Paikallaan ollessa taas oli päästy käsiksi ovien lukitukseen, kattoluukkuun ja valoihin. Kokeen tekijät lähettivät tuloksensa Teslalle. Autoihin tuli haavoittuvuuden korjaava päivitys vain kymmenen päivää siitä, kun haavoittuvuudesta oli ilmoitettu valmistajalle.

4.3 Tulevaisuuden näkymiä ja edotettuja ratkaisuja

Kuten aikaisemmin esitellyistä esimerkeistä näkyy, voidaan jo nyt kyberhyökkäyksillä tehdä suurta vahinkoa henkilöautoille ja niillä liikkuville. Kuitenkin suurin osa tiedossa olevista tapauksista ovat olleet suunniteltuja ja testimielessä toteutettuja. Monet varoittavat kuitenkin siitä, että tulevaisuudessa mielenkiinto autoihin kohdistuvia kyberhyökkäyksiä kohtaan tulee lisääntymään (Iqbal, Haque ja Zulkernine 2019; Levi, Allouche ja Kontorovich 2018).

Sekä autojen ohjelmistojen määrä, että ylipäätään yhdistettyjen autojen määrä ovat olleet suuressa kasvussa viime vuosina ja kasvun voi olettaa vain kasvavan entisestään. Burkacky ym. (2018) kertovat kuinka esimerkiksi vuodesta 2010 vuoteen 2016 yksittäisen modernin auton sisältämä koodin määrä on kasvanut noin kymmenestä miljoonasta jopa 150 miljoonaan riviä koodia. Tästä on helppo päätellä, että myös mahdollisten heikkouksien määrä on valtavassa kasvussa. Erilaisia hyökkäysvektoreita syntyy koko ajan lisää eri puolille autoja. He muistuttavatkin siitä, kuinka autovalmistajien ja varsinkin ohjelmistojen tekijöiden olisi tärkeää ottaa huomioon myös ohjelmistoturvallisuus.

Iso haaste autojen tietokoneissa on niiden ikä. Samalla autolla voidaan ajaa helposti jopa 20 vuotta. Jokainen voi miettiä miten paljon tietokoneet ovat kehittyneet vaikkapa edellisen kymmenen vuoden aikana. Lisäksi laitteiden tehoon vaikuttaa se, että niiden täytyy olla kestäviä muun muassa tärinän ja kosteuden takia. Vanhentuneiden järjestelmien pitää pystyä puolustautumaan valtavan laskentatehon sisältävien tietokoneiden tuottamia hyökkäyksiä (Onishi 2012). Onkin hyvin mahdollista, että tästä tulee suurempikin ongelma muutama vuoden päästä, kun isosti yleistyvien yhdistettyjen autojen tekniikka alkaa vanhentua.

Suojautumiseen haittaohjelmia vastaan on ehdotettu monia vaihtoehtoja. Monia näistä keinoista yhdistää se, että auton sisäistä ja ulkoista liikennettä pitää valvoa ja valvonnan kautta pyrkiä tunnistamaan haittaohjelmat ajoissa. Esimerkiksi Levi, Allouche ja Kontorovich (2018) esittelevät ratkaisua, jossa heidän järjestelmänsä ei valvo pelkästään CAN-väylää, vaan myös esimerkiksi käyttöjärjestelmää ja tietoverkkoa. Ideana olisi se, että vaikka jostain kerroksesta ja teknologiasta päästäisiin haittaohjelmalla läpi, olisi vähintään tieto siitä auton kuljettajalla ennen, kuin haittaohjelma pääsisi vaikuttamaan kriittisiin osiin, kuten vaikkapa jarrujen toimintaan. Myös Onishi (2012) ehdottaa vastaavaa ja hän korostaakin itsediagnoo-

sia, itsetunnistusta ja itsevaroitusta tärkeinä ominaisuuksina autoissa. Hän myös muistuttaa miten tärkeää näiden olisi toimia nopeasti tartunnan saamisen jälkeen, jotta vakavilta onnettomuuksilta vältytään.

Onishi (2012) kertoo myös, että tärkeää olisi valmistautua tilanteeseen, jossa tartunta on jo päässyt leviämään kriittisiin komponentteihin. Esimerkiksi jarrut, moottorin sammuttaminen ja ovien avaaminen sisältä päin pitäisi toimia, vaikka kyseisiin laitteistoihin olisikin päässyt tunkeutumaan haittaohjelma. Kaiken tämän lisäksi on tietysti erittäin tärkeää kehittää yksittäisten komponenttien omaa suojausta. Esimerkiksi CAN-väylän kehittämistä ei voi missään nimessä unohtaa.

5 Yhteenveto

Nykyaikaisessa henkilöautossa on valtava määrä eri teknologioita ja ohjelmistoja ja määrä on koko ajan vain kasvussa. Jokainen uusi teknologia tai ohjelmisto on uusi mahdollinen heikkous kyberturvallisuuden näkökulmasta. Näitä heikkouksia löytyy kaiken aikaa ja tulee tulevaisuudessa varmasti löytymään lisää. Tietynlainen standardien puute tekee autojen kyberturvallisuuden kehittämisestä hankalampaa. Valtava kehitys toisaalta myös pakottaa valmistajia kiirehtimään uusia järjestelmiään valmiiksi ja harmillisesti tällöin saattaa nimenomaan kyberturvallisuus olla osa-alue, joka jää vähemmälle huomiolle.

Autoihin kohdistuvat kyberhyökkäykset ovat olleet toistaiseksi melko vähäisiä. Suurin osa löytyneistä tapauksista oli toteutettu testi mielessä, jotta esimerkiksi autovalmistajat saataisiin ottamaan kyberturvallisuus tarpeeksi vakavasti ja kehittämään autojen turvallisuutta myös ohjelmistojen puolella. Tällä hetkellä tapahtuvat varsinaiset hyökkäykset ovat olleet lähinnä autojen varastamista lukitusta manipuloimalla tai muuten välitöntä vaaraa aiheuttavia. Kuitenkin testeissä on onnistuttu jopa pysäyttämään autoja keskelle liikennettä. Lisäksi hyökkäysten toteuttaminen on usein erittäin halpaa, joten tämäkään ei estä hakkereita toteuttamasta ideoitaan.

Hyökkäyksiä tulee varmasti tulevaisuudessa olemaan enemmän kuin mitä on tähän mennessä nähty. Voidaan vain kuvitella mitä tuhoa syntyy, kun itseajavat autot yleistyvät ja valtaavat katunäkymät ja joku onnistuu hakkeroitumaan näiden autojen järjestelmiin. Puhumattakaan kaikista muista ajoneuvoista mitä maailmastamme jo nyt löytyy. Lentokoneesta sähköpotkulautaan voidaan aiheuttaa hyvin paljon erilaista ja eri vakavuus asteen vahinkoja ajoneuvojen käyttäjille.

Kyberturvallisuuden parantamiseen on ehdotettu monia vaihtoehtoja. Usein kuitenkin korostetaan sitä, että jokainen yksikkö on suojattava erikseen ja toivottavasti näin autojen kehityksessä myös tapahtuu. Myös testi mielessä toteutetut hyökkäykset ovat tärkeä osa turvallisuuden kehitystä, sillä silloin valmistajat näkevät miten helposti heidän järjestelmistänsä voidaan löytää heikkouksia.

Lähteet

Bajpai, Pranshu, Richard Enbody ja Betty HC Cheng. 2020. “Ransomware targeting automobiles”. Teoksessa *Proceedings of the Second ACM Workshop on Automotive and Aerial Vehicle Security,* 23–29.

Bécsi, Tamás, Szilárd Aradi ja Péter Gáspár. 2015. “Security issues and vulnerabilities in connected car systems”. Teoksessa *2015 International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS),* 477–482. IEEE.

Burkacky, Ondrej, Johannes Deichmann, Georg Doll ja Christian Knochenhauer. 2018. “Rethinking car software and electronics architecture”. *McKinsey & Co., February.*

Charette, Robert N. 2009. “This car runs on code”. *IEEE spectrum* 46 (3): 3.

Coppola, Riccardo, ja Maurizio Morisio. 2016. “Connected car: technologies, issues, future trends”. *ACM Computing Surveys (CSUR)* 49 (3): 1–36.

Iqbal, Shahrear, Anwar Haque ja Mohammad Zulkernine. 2019. “Towards a security architecture for protecting connected vehicles from malware”. Teoksessa *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring),* 1–5. IEEE.

Levi, Matan, Yair Allouche ja Aryeh Kontorovich. 2018. “Advanced analytics for connected car cybersecurity”. Teoksessa *2018 IEEE 87th Vehicular Technology Conference (VTC Spring),* 1–7. IEEE.

Newcomb, Deug. 2012. “The Next Big OS War Is in Your Dashboard”. *Wired.*

Nie, Sen, Ling Liu ja Yuefeng Du. 2017. “Free-fall: Hacking tesla from wireless to can bus”. *Briefing, Black Hat USA* 25:1–16.

Onishi, Hiro. 2012. “Paradigm change of vehicle cyber security”. Teoksessa *2012 4th International Conference on Cyber Conflict (CYCON 2012),* 1–11. IEEE.

Ring, Tim. 2015. “Connected cars–the next target for hackers”. *Network Security* 2015 (11): 11–16.

Woo, Samuel, Hyo Jin Jo ja Dong Hoon Lee. 2014. “A practical wireless attack on the connected car and security protocol for in-vehicle CAN”. *IEEE Transactions on intelligent transportation systems* 16 (2): 993–1006.

Zhang, Tao, Helder Antunes ja Siddhartha Aggarwal. 2014. “Defending connected vehicles against malware: Challenges and a solution framework”. *IEEE Internet of Things journal* 1 (1): 10–21.