



Tietoturva auton sisäisissä CAN-verkoissa

Oulun yliopisto
Tieto- ja sähkötekniikan tiedekunta
Tietojenkäsittelytieteiden tutkinto-
ohjelma
LuK-tutkielma
Sampsa Jalli
27.6 2019

Tiivistelmä

Tämä tutkielma käsittelee autojen sisäisten CAN-verkkoja sekä niihin liittyviä tietoturvakysymyksiä. Tutkielmassa käsitellään autoissa yleisesti käytetyn CAN-väyläjärjestelmän perusteita, historiaa sekä myös autojen tietoturvaan liittyviä periaatteita teoreettisella tasolla tasolla. Tämän jälkeen tarkastellaan jo olemassa olevan kirjallisuuden ja tutkimuksen pohjalta CAN-väylään liittyviä konkreettisia tietoturvaongelmia, sekä joissain tapauksissa myös tapoja, joilla niitä voidaan poistaa tai vähentää. Tutkielmassa pohditaan myös tietoturvan merkitystä autoissa, sekä sen mahdollisia suuntauksia autoteollisuudessa tulevaisuudessa.

Asiasanat

Autot, ajoneuvot, CAN-verkot, tietoturva

Ohjaaja

Mari Karjalainen

Sisällys

1. Johdanto.....	4
2. Keskeiset käsitteet.....	6
2.1 Autojen tietoturva.....	6
2.2 Auton CAN-väylä.....	7
3. CAN-väylän tietoturvasuus.....	10
3.1 Fyysiset hyökkäykset.....	10
3.2 Epäsuorat hyökkäykset.....	12
4. Tietoturvan parantaminen.....	14
4.1 Komponenttien kryptografinen varmennus.....	14
4.2 Epätavallisten CAN-viestien tunnistaminen ja/tai suodattaminen.....	15
5. Pohdinta.....	17
6. Yhteenveto.....	18
7. Lähdeluettelo.....	19

1. Johdanto

Vaikkakin ulkonäöllisesti autot ovat pysyneet suurelta osin melko muuttumattomina vuosien varrella, sisäisten komponenttien tasolla ne ovat käyneet läpi paljon muutoksia 1900-luvun lopulla ja 2000-luvulle tultaessa. Suurimpia näistä muutoksista on ollut mikroprosessorien käyttö autoissa, mikä alkoi kuluttajille myytävissä ajoneuvoissa vuonna 1978 (Cook, Kolmanovsky, McNamara, Nelson & Prasad, 2007). Lukumäärä on vuosien varrella vain kasvanut, ja nykyautosta löytyy valmistajasta ja mallista riippuen kahdestakymmenestä kahdeksaankymmentä mikroprosessoria (Cook et al., 2007). Niiden avulla on korvattu esimerkiksi auton sisäisiä mekaanisia kontrolliväyliä sähköisillä, jolloin ne auttavat tehostamaan tai lisäämään auton osien välistä sisäistä kommunikaatiota (Cook et al., 2007). Mikroprosessorit ja sähköiset kontrolliyksiköt ovat myös mahdollistaneet monia luksusominaisuuksiksi luokiteltavia toiminnallisuuksia, kuten esimerkiksi sähköisesti toimivat ikkunat tai erilaisten mediantoistojärjestelmien liittäminen osaksi auton ohjaamaa (Cook et al., 2007; Bosch, 2014).

Teknologian kehittyessä autot ovat alkaneet olla enemmän ja enemmän riippuvaisia siitä, että nämä sähköiset komponentit, niiden käyttämät kommunikaatioväylät ja -protokollat toimivat juuri niin kuin niiden pitääkin, ilman ongelmia. Tähän liittyvät monella tavalla samat kysymykset, joita on jo käsitelty liittyen muuhun kuluttajaelektroniikkaan, kuten älypuheliiniin ja tietokoneisiin. Tietoturva ja käyttäjien yksityisyys ovatkin keskeisiä puheenaiheita nykyaikana. Sillä vaikka autojen valmistajat ovatkin vuosien saatossa kehittäneet autojen turvallisuutta paremmaksi esimerkiksi kolareissa, autojen turvallisuus tilanteissa, joissa pahantahtoinen toimija yrittää tunkeutua järjestelmään ja aiheuttaa vaaratilanteita, on vielä suurelta osin alue, jossa parantamisen varaa on paljon (Wolf, Weimerskirch & Wollinger, 2006; Larson & Nilsson, 2008; Islam, Lautenbach, Sandberg & Olovsson, 2016).

Ottaen huomioon henkilöautojen, sekä ajoneuvojen ylipäätänsä, keskeisen aseman modernissa yhteiskunnassa työkaluina, niiden sisäisten tietoverkkojen haavoituvuuksien ja ongelmien tarkasteleminen on hyvin tärkeää, erityisesti ottaen huomioon 2000-luvulla tapahtuneen kehityksen IoT-laitteissa ja itseajavissa autoissa (Koushanfar, Sadeghi & Seudie, 2012). Siispä halu ja työkalut etsiä ongelmia ja korjata ne ovat kriittisiä autojen ja niiden sisäisen elektroniikan, sekä myös liikenteen toimivan tulevaisuuden kannalta.

Tämän tutkielman tarkoituksena on tarkastella tiettyä autoista löytyvää sisäistä tietoverkkoa: CAN-väylää, joka on autoissa yleisesti käytetty väyläjärjestelmä, joka yhdistää auton sisäiset komponentit, kuten mikroprosessorit ja elektroniset kontrolliyksiköt, toisiinsa (Lawrenz, 2013; Bosch, 2014). Väyläjärjestelmän yleisen kuvauksen lisäksi tutkielmassa tarkastellaan CAN-väylän tietoturvaa sekä fyysisiä että epäsuoria hyökkäyksiä vastaan. Lopuksi nostetaan esille mahdollisia keinoja korjata löytyneitä ongelmia. Tutkielman on kirjallisuuskatsaus, eli siinä käsitellään jo olemassa olevaa tutkimusta ja kirjallisuutta aiheesta ja niistä saatua tietoa.

Tässä kirjallisuuskatsauksessa lähteiden hakemiseen käytettiin laajasti erilaisia tietokantoja: Scopusta yleiseen aiheen kartoitukseen, ja IEEE Xploria, ACM Digital Librarya sekä SpringerLinkiä tarkempiin hakuihin. Käytetyt hakusanaketjut hauissa olivat seuraavanlaiset: ("CAN bus" AND security) ja ("Attack surface" AND ("car" OR "vehicle" OR "automotive")) Rajaavina tekijöinä artikkeleiden suhteen keskityttiin

paljolti julkaisuvuoteen ja siteerausten määrään, joiden pohjalta pyrittiin poimimaan 2000- ja 2010-luvuilla tehtyjä artikkeleita, jotta ne olisivat mahdollisimman relevantteja tarkastellun aiheen kannalta.

Suurin varsinainen rajausta, joka aihepiiriä käsiteltäessä tehtiin, oli liittyen itseajaviin autoihin, jotka suljettiin tarkasteltavan alueen ulkopuolelle. Tämä päätös tehtiin pääosin siksi, että itseajavat autot ovat vielä suurelta osin kehittyvä osa autoteollisuutta ja IT-teknologiaa, eivätkä vielä yhtä laajassa käytössä maailmalla. Kuitenkin myös tulevaisuuden kannalta tämän aihepiirin tutkiminen tarkemmin sekä teoriatasolla että myös kvalitatiivisella tutkimuksella olisi hyvä idea lähitulevaisuudessa, jotta myös itseajavien autojen ongelmista saataisiin kerättyä tieteellistä tietoa.

2. Keskeiset käsitteet

2.1 Autojen tietoturva

Ajoneuvoihin liittyvä tietoturva on konseptina melko uusi. Kuitenkin sitä voidaan tarkastella jo olemassa olevien konseptien ja keinojen avulla, jotka pätevät jo olemassa oleviin laitteisiin, kuten pöytätietokoneisiin tai älypuhelimisiin. Tällainen on esimerkiksi niin kutsuttu CIA:n kolmio, jota on jo pitkään käytetty ohjenuorana tietoturvassa määrittämään ne kolme keskeistä konseptia, jotka hyvässä tietoturvassa tulisi täyttyä (Whitman & Mattord, 2011). Kirjassaan Whitman ja Mattord (2011) määrittävät tämän kolmion sisällön seuraavasti:

- 1) Confidentiality eli luotettavuus. Informaatiojärjestelmän voidaan sanoa täyttävän tämän vaatimuksen, kun sen sisältämään tietoon pääsevät käsiksi vain ne, joilla on siihen lupa.
- 2) Integrity eli koskemattomuus. Tämä vaatimus täyttyy, kun voidaan varmuudella sanoa tai varmistaa, että informaatio ei ole korruptoitunut esimerkiksi siirron aikana, tai muuten luvattomasti muokattu kolmannen osapuolen toimesta.
- 3) Availability eli saatavuus. Informaation tulisi olla saatavilla niille, joille sen käsittelyyn on annettu lupa.

Othmane et al. (2015) tekemässä tutkimuksessa määritellään erilaisia uhkatyyppejä, joita verkon avulla yhdistettyihin autoihin saatetaan kohdistaa sen mukaan, millaisia vaikutuksia niillä on. Tällaisia voivat olla esimerkiksi uhat, jotka vaikuttavat käyttäjään tai auton valmistajaan taloudellisesti, jos tunkeutuja tai salakuuntelija pystyy esimerkiksi hyödyntämään auton järjestelmissä kulkevaa ja niistä lähetettävää tietoa rahallisesti. Tähän liittyy vahvasti myös uhat, jotka vaarantavat käyttäjän yksityisyyden, jos kolmansilla osapuolilla on mahdollisuus päästä käsiksi tietoihin. Kolmantena ja viimeisenä ovat suoraan turvallisuuteen vaikuttavat uhat, kun hyökkääjä tarkoituksella pääsee vaikuttamaan kriittisiin turvallisuuteen vaikuttaviin komponentteihin, kuten jarruihin.

Käyttäen aikaisemmin määriteltyä CIA-kolmiota (Whitman & Mattord, 2011), sen avulla voidaan tarkastella Othmane et al. (2015) määrittelemiä uhkatyyppejä ja niiden suhdetta jo olemassa oleviin tietoturvan tärkeisiin osa-aleisiin.

Kun autojen CAN-verkkojen sisäistä tietoturvaa tarkastellaan edellä määriteltyjen tietoturvan konseptien pohjalta, voidaan havaita selviä puutteita kaikkien kolmen periaatteen suhteen. Johtuen CAN-väylän luonteesta ja suunnitteluperiaateista, luotettavuus ei ole saavutettavissa, koska broadcast-periaatteen ja viestien salaamattomuuden takia kaikki viestit ovat kaikkien verkossa olevien solmujen luettavissa (Kleberger, Olovsson, & Jonsson, 2011; Buttigieg, Farrugia & Meli, 2017; Bozdal, Samie & Jennions, 2018). Ainoa varsinainen virheentarkistukseen käytetty toiminto CAN-viesteissä on CRC-kenttä, joka sisältää 16-bittisen syklisen redundanssitarkistuksen (Bosch, 2014). Tämä ei kuitenkaan varsinaisesti auta varmistamaan viestien koskemattomuutta, vaan sen avulla varmistetaan, onko viestin sisältö mahdollisesti korruptoitunut (Carsten, Andel, Yampolskiy & McDonald, 2015;

Farrugia et al., 2017; Bozdal et al., 2018). Myöskään saatavuus ei ole saavutettavissa johtuen CAN-väylän arbitraatiosääntöjen toiminnan takia, joissa korkeamman prioriteetin solmuille annetaan etuoikeus lähettää viestejä väylässä (Bosch, 2014; Bozdal et al., 2018). Jos korkeamman prioriteetin solmu väylässä lähettää viestejä koko ajan, se käytännössä lukitsee alemman prioriteetin solmut ulos ja pakottaa ne odottamaan kunnes ne voivat lähettää oman viestinsä, täten rikkoen CIA kolmion viimeistä kohtaa (Bozdal et al., 2018).

2.2 Auton CAN-väylä

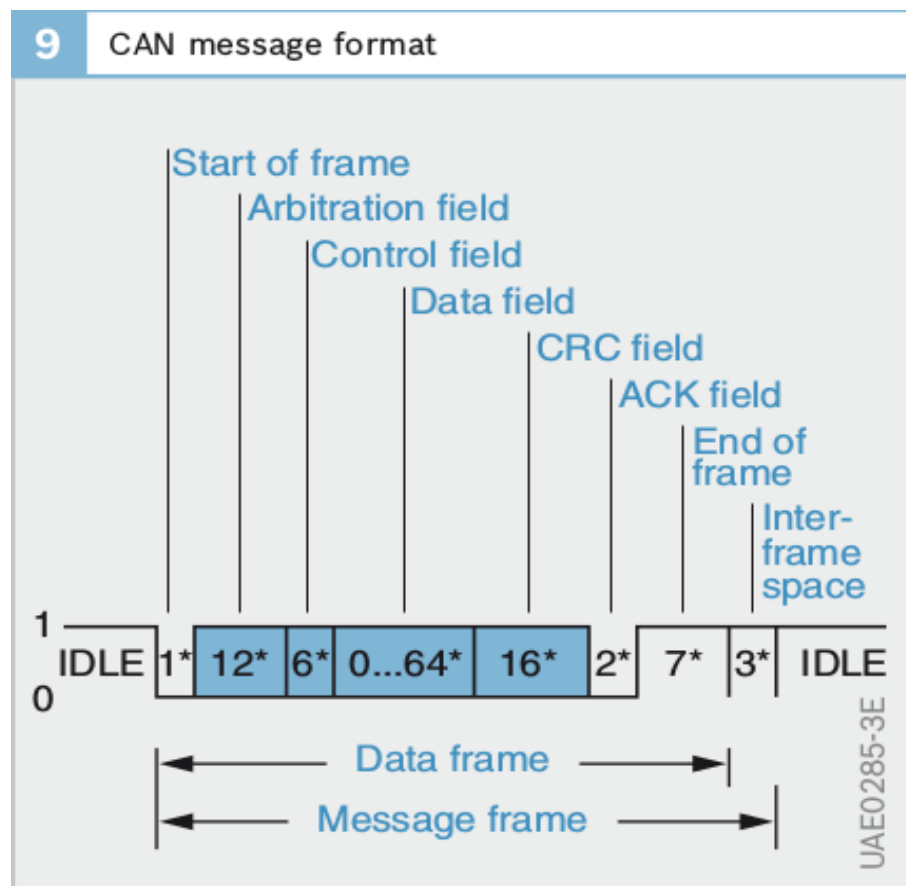
Controller Area Network (CAN) -väylä on ISO 11898 standardissa määritelty väyläjärjestelmä, joka otettiin käyttöön ensimmäisissä massatuotetuissa ajoneuvoissa vuonna 1991. Tämän väyläjärjestelmän tarkoituksena on yhdistää auton sisällä olevat sähköiset kontrolliyksiköt (Electronic Control Unit, ECU) toisiinsa, ja mahdollistaa viestien kuljettaminen niiden välillä (Lawrenz, 2013; Bosch, 2014).

Topologiaaltaan CAN-väylä suunniteltiin olemaan mahdollisimman vähän riippuvainen keskitetystä kontrolliyksiköstä, minkä takia käytettäväksi valikoitui lineaarinen väylätopologia, jossa kaikki järjestelmän kautta yhteydessä olevat laitteet ovat kiinni samassa väylässä (Lawrenz, 2013; Bosch, 2014). Tämä mahdollistaa sen, että rikkinäinen kontrolliyksikkö ei helposti pysty aiheuttamaan ongelmia väylälle kokonaisuutena, sekä myös sen, että uusien komponenttien lisääminen on mahdollisimman helppoa (Lawrenz, 2013; Bosch, 2014). Tämän lisäksi viestit CAN-väylässä lähetetään broadcast periaatteella: viesteissä ei ole erillistä kenttää lähettäjälle ja vastaanottajalle, minkä takia CAN-viestit lähetetään koko väylän laajuisesti, ja kaikki väylässä kommunikoivat laitteet pystyvät lukemaan ne. Se, mitkä viestit vastaanotetaan, riippuu laitteiden omasta sisäisestä logiikasta ja suodattimista (Lawrenz, 2013; Bosch, 2014).

ISO 11898 standardi jakaa CAN-väylän tukemat nopeudet kahteen erilliseen luokkaan, joita on yhteensä kaksi. Ensimmäinen näistä on korkean nopeuden CAN (CAN-C), jonka nopeus vaihtelee sijoittuu välille 125 kBit/s – 1Mbit/s (Lawrenz, 2013; Bosch, 2014). CAN-C:tä käytetään kuljettamaan tietoa esimerkiksi moottoria ja vaihteistoa kontrolloivien järjestelmien välillä. Toinen määritelty on matalan nopeuden CAN (CAN-B), jonka nopeus vuorostaan on väliltä 5 – 125 kBit/s (Lawrenz, 2013; Bosch, 2014). Sitä käytetään vähemmän kriittisten osien hallintaan ja näiden osien väliseen kommunikaatioon, kuten sähköisten ikkunoiden, ilmastoinnin tai sähköllä toimivien penkkien hallinnoimiseen (Bosch, 2014).

CAN-väylässä liikkuvien viestien formaatteja on olemassa kahta erilaista: standardi CAN 2.0 A, ja pidennetty CAN 2.0 B. Erottava tekijä näiden kahden välillä on tunnisteessa käytetty tavujen määrä, joka on standardissa 11 bittiä, ja 29 bittiä pidennetyssä, muuten ne ovat sisällöltään samanlaisia. Kommunikaatioon CAN-väylä käyttää kahta erilaista loogista tilaa, joiden avulla bitit muodostetaan: dominoiva, joka vastaa binääristä arvoa nolla, ja resessiivinen, joka puolestaan vastaa binääristä arvoa yksi (Lawrenz, 2013; Bosch, 2014).

Bosch (2014) määrittelee normaalin CAN-viestin sisältävän seuraavat kentät:



Kuva 1. CAN-viestin rakenne (Bosch, 2014)

Viestikehyksen alku: pituudeltaan yksi bitti, sen tarkoituksena on merkitä kehyksen alkamispaikka.

Arbitraatiokenttä: sisältää tunnusteen, standardissa 11 bittiä pitkä, pidennetyssä 29. Tapauksissa, joissa monta eri osapuolta yrittää lähettää viestin samanaikaisesti, tunnusteen avulla lasketaan, millä viestillä on korkein prioriteetti. Mitä pienempi tunnusteen arvo, sitä korkeampi viestin prioriteetti on.

Kontrollikenttä: CAN-A:ssa sisältää kuusi bittiä, joista ensimmäinen on Identifier Extender Bit (IDE), jolla viesti tunnustetaan CAN-A:han kuuluvaksi. Toinen bitti on ”varalla”, eikä sitä varsinaisesti käytetä. Viimeiset neljä bittiä kertovat, kuinka paljon dataa seuraavassa kentässä on.

Datakenttä: Sisältää viestissä lähetetyn tiedon, ja on pituudeltaan maksimissaan 64 bittiä. Lähetetyn viestin datakenttä voi olla myös 0 bittiä pitkä, jolloin sitä voidaan käyttää hajautettujen prosessien synkronointiin.

CRC-kenttä: Sisältää syklisen redundanssitarkistuksen, joka on 16 bittiä pitkä tarkistussumma, jonka avulla voidaan laskea, onko vastaanotetussa viestissä ollut virheitä.

ACK-kenttä: Kenttä, jonka pituus on kaksi bittiä. Vastaanottaja käyttää sitä kuittaamaan saamansa viestin vastaanotetuksi uudelleenlähettämällä saamansa viestin ja muuttamalla ACK-kentän arvon.

Kehyksen loppu: Seitsemän perättäistä resessiivistä bittiä, joilla ilmaistaan viestikehyksen päätyminen.

Kehysten välinen tila: Lähetettyä viestiä seuraavat resessiiviset bitit, jotka määrittävät ikkunan koon, jonka jälkeen muut voivat lähettää viestejä.

Selkeyden vuoksi on tässä katsauksessa CAN-viestin sisältö yllä esitelty kokonaisuudessaan. Kuitenkin lopulta tarkastellun aiheen kannalta kiintoisimmat ja merkityksellisimmät kentät ovat arbitraatio-, kontrolli- ja datakentät. Tunkeutujan lähettäessä viestejä väylässä arbitraatiokenttä mahdollistaa lähettäjän omien viestien prioriteetin kasvattamisen, ja jos viestejä lähetetään tarpeeksi suurella frekvenssillä, pakottaa tämä muut solmut odottamaan (Bozdalet al., 2018). Datakenttä taas sisältää lähetettävät komennot tai tilatiedot, joista hyökkääjä voi olla kiinnostunut halutessaan vaikuttaa muiden väylässä olevien solmujen toimintaan haitallisesti.

3. CAN-väylän tietoturvallisuus

Jo suunnitteluperiaatteidensa takia CAN-väylää pitkin lähetettyjen viestien tietoturva altistuu vaaratekijöille. CAN-viesteissä ei ole olemassa kenttää lähettäjälle tai vastaanottajalle, vaan kaikki verkossa olevat solmut, jotka kykenevät paketin lukemaan, lukevat sen (Carsten et al., 2015; Buttigieg et al., 2017). Tästä seuraa myös se, että CAN-väylässä liikkuvia viestejä on mahdotonta autentikoida täysin, koska yksikään verkossa oleva solmu ei kykenee todentamaan, mistä viesti tarkalleen ottaen on tullut (Carsten et al., 2015; Buttigieg et al., 2017). Näistä johtuen ei myöskään pystytä aukottomasti todentamaan sitä, että kaikki verkkoon yhdistetyt solut olisivat aitoja, joka nostaa hyökkäyksen riskiä, jossa kaapattu solmu lähettää väärennetyjä viestejä toisille (Carsten et al., 2015; Buttigieg et al., 2017).

Tässä tutkielmassa hyökkäykset CAN-väylän tietoturvaa vastaan on jaettu kahteen eri tyyppiin: fyysiset hyökkäykset, jotka vaativat hyökkääjää olemaan suoraan yhdistettynä autoon, sekä epäsuorat hyökkäykset, jotka voidaan suorittaa ilman, että suoraa yhteyttä autoon esimerkiksi fyysisen johdon avulla tarvittaisiin.

3.1 Fyysiset hyökkäykset

Suorista fyysisistä hyökkäysmetodeista CAN-väylää vastaan yksinkertaisin on käyttää hyväksi autosta löytyvää On Board Diagnostics II (OBD) -porttia, jota normaalisti käytetään huoltodiagnostiikan keräämiseen korjaamoissa (Hoppe, Kiltz & Dittmann, 2008; Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H. & Savage, S., 2010; Carsten et al., 2015). OBD II-portit ovat erittäin laajasti käytössä nykyautoissa, ja esimerkiksi Yhdysvalloissa on liittovaltiotasolla säädetty laki, jonka mukaan diagnostiikkaportti on pakollinen kaikissa uusissa autoissa (Carsten et al., 2015).

Yksi ensimmäisistä dokumentoiduista onnistuneista hyökkäyksistä CAN-väylän tietoturvaa vastaan oli Hoppe ja Dittmanin (2006) suorittamassa kokeessa, joka kohdistui simuloituun auton sähköikkunaan (Bozdal et al., 2018; Groza & Murvay, 2018). Myöhemmin Koscher et al. (2010) toteuttamassa kokeessa testattiin empiirisesti, kuinka altis testattavan auton sisäinen tietoverkko on mahdolliselle fyysiselle hyökkäykselle, eli tehtiin oletus tilanteesta, jossa hyökkääjä kykenee suoraan muodostamaan yhteyden järjestelmään hallussaan olevan laitteen avulla. Kokeessa käytetty pääasiainen hyökkäyspinta oli testattavan auton OBD II-portti, ja hyökkäyksen toteuttamiseen käytettiin kannettavaa tietokonetta, johon oli asennettu CAN-pakettien urkkimiseen tarkoitettu ohjelma, ja kannettava tietokone itsessään oli yhdistetty kaapeleilla OBD II -porttiin.

Kuten jo aikaisemmin todettiin, CAN-väylää itseään ei ole millään tavalla suojattu urkkimiselta, koska topografiansa ja toimintaperiaatteensa takia kaikki yhdistetyt laitteet kykenevät periaatteessa vastaanottamaan kaikki väylässä kulkevat viestit (Bosch, 2014; Carsten et al., 2015). Ainoastaan yhdistettyjen komponenttien oma sisäinen logiikka vastaa siitä, mitä paketteja ne lukevat ja mitä eivät, ja tästä johtuen kartan muodostaminen testattavan auton sisäisestä CAN-verkosta kokeen aikana oli erittäin helppoa (Koscher et al., 2010).

Koscher et al., (2010) sovelsi tutkimuksissaan myös fuzzausta, joka on tietoturvan testauksessa käytetty metodi, jossa järjestelmälle annetaan satunnaisia syötteitä. Yllättävä löydös kokeen aikana oli, että jo pelkästään käyttämällä fuzzausta CAN-viesteihin pystyttiin luomaan väärennettyjä viestejä jotka järjestelmä hyväksyi, pääosin johtuen validien CAN-viestien pienestä koosta, joka tekee satunnaisesta viestien väärentämisestä tällä tavalla todennäköisempää ja helpompaa (Koscher et al., 2010).

Koetta suorittaessaan Koscher et al. (2010) löysivät myös standardeista poikkeavia käytäntöjä testatuista komponenteista, jotka altistivat ne normaalia vaarallisemmille hyökkäyksille. Tällainen oli esimerkiksi komento kytkeä CAN-kommunikaatio pois päältä, jonka kontrolliyksikön tulisi hylätä sellaisissa tapauksissa, joissa sen suorittaminen on vaarallista, kuten silloin kun auto on liikkeessä (Koscher et al., 2010). Toinen esimerkki oli komento poistaa tai asentaa uudelleen kontrolliyksikön ohjaava laiteohjelmisto, joka myös hyväksyttiin tilanteessa, jossa se olisi pitänyt automaattisesti hylätä (Koscher et al., 2010). Huomioitavaa on kuitenkin se, että kyseessä oleva ongelma esiintyi vain testatussa autossa (Koscher et al., 2010), eikä siis ole selvää kuinka yleisiä mainittujen kaltaiset virheet ovat esimerkiksi sähköisten kontrolliyksiköiden koodissa.

Väärennettyjen CAN-viestikäskyjen lisäksi on onnistuneesti testattu myös metodeja, joissa väylään injektoidaan ainoastaan tilasta kertovia viestejä (Takahashi, Tanaka, Fuji, Narita, Matsumoto, & Sato, 2018). Takahashi et al. (2018) suorittamassa kokeessa onnistuttiin huijaamaan auton vakionopeudensäädintä kiihdyttämään lähettämällä sille väärennettyjä tilapäiviyysviestejä, joilla se huijattiin luulemaan, että auton tilannenopeus oli matalampi kuin ajajan vakionopeudeksi asettama arvo. Vaikkakin kuvaillun kaltainen tilatiedon väärentämiseen perustuva hyökkäys ei olekaan välttämättä yhtä vaarallinen kuin esimerkiksi Koscher et al. (2010) kuvaamat ja testaamat keinot, saattaa yhtäkkinen nopeuden nouseminen aiheuttaa vaaratilanteen, jos kuljettaja ei huomaa sitä tai jarruttaa yhtäkkiä vähentääkseen kasvanutta nopeutta (Takahashi et al., 2018).

On löydetty myös hyökkäystekniikoita, jotka hyödyntävät CAN-väylän omia virreehallinnan työkaluja sitä itseään vastaan. Tällainen on niin kutsuttu ”bus-off” -hyökkäys, jossa hyökkääjä huijaa väylässä kiinni olevan sähköisen kontrolliyksikön luulemaan, että sen lähetämät viestit ovat virheellisiä, jolloin se sulkee itsensä pois väylän kommunikatiosta turvallisuussyistä ja siirtyy ”bus-off” -tilaan. (Cho & Shin, 2016). Hyökkäys perustuu kohteena olevan sähköisen kontrolliyksikön sisäisen TEC (Transmission Error Counter) tai REC (Receive Error Counter) -arvojen kasvattamiseen: virheellisen viestin lähettäminen nostaa arvoa kahdeksalla, kun taas virheetön viesti laskee sitä yhdellä (Cho & Shin, 2016). Kun nämä arvot nousevat tarpeeksi korkeiksi (>255), kontrolliyksikkö siirtyy bus-off -tilaan (Cho & Shin, 2016). Sen lisäksi, että hyökkääjän pitää pystyä lähettämään viestejä väylässä (Esimerkiksi toisen sähköisen kontrolliyksikön avulla, johon hyökkääjällä on pääsy), on hänen myös hyökkäyksen onnistumiseksi tiedettävä myös kohteena olevan sähköisen kontrolliyksikön tunnus, jolla se lähettää viestejä sekä tieto siitä, kuinka usein se lähettää viestejä (Cho & Shin, 2016). Viimeisenä hyökkääjän tarvitsee varmistaa, että hänen samaan aikaan lähettämänsä viestin sisältö eroaa kohteen viestistä siten, että hyökkääjän viestissä on ainakin yksi dominoiva (0) bitti, joka hyökkäyksen kohteella on resessiivinen (1): kun nämä viestit lähetetään samanaikaisesti, hyökkääjä pakottaa kohteelle bittivirheen, joka nostaa sen TEC-arvoa kahdeksalla (Cho & Shin, 2016). Johtuen tästä erosta TEC-arvon kasvattamisen ja laskemisen välillä, on mahdollista saada kohteena oleva sähköinen kontrolliyksikkö bus-off -tilaan, vaikka hyökkääjä keskittyyisikin vain yhteen viestityyppiin, jota kohde lähettää (Cho & Shin, 2016).

Suurimmat käytännön ongelmat, jotka Cho ja Shin (2016) nostivat tutkimuksessaan esille, ovat kohteen viestitunnisteen selvittäminen, viestin sisällön varmistaminen siten,

että se aiheuttaa bittivirheen, sekä viestin lähettämisen synkronointi siten, että se on samanaikainen uhrin kanssa. Koska CAN-väylässä olevat viestit lähetetään siten, että kaikki väylässä olevat pystyvät ne lukemaan, tämä on suurelta osin triviaalia, ja suurimmaksi esteeksi jäävät sähköisten kontrolliyksiköiden omat sisäiset suodattimet, joiden avulla ne päättävät, mitä viestejä ne vastaanottavat (Cho & Shin, 2016).

Koska kohteena olevan sähköisen kontrolliyksikön lähettämän viestin sisältöä ei voida varmasti täysin tietää, on valittava se osa siitä, jonka hyökkääjä voi suurimmalla varmuudella saada väärin tarkoituksella (Cho & Shin, 2016). Yksi varma tapa on asettaa viestin DLC (Data Length Code) -kentän arvo nolllaksi, koska suurimmassa osassa CAN-viestejä tämä arvo on nolllaa suurempi (Cho & Shin, 2016). Viestin lähettämisen synkronointi on vaikein näistä aikaisemmin mainitusta kolmesta, kuitenkin jos kohteen tiedetään lähettävän tiettyjä viestejä tietyllä frekvenssillä, voidaan oman viestin lähettämisaika yrittää ajoittaa oikeaksi tämän tiedon perusteella (Cho & Shin, 2016).

Kiintoisan tästä hyökkäystekniikasta tekee se, että se perustuu CAN-protokollan omien sisäisten virreehallintarakenteiden ja logiikan hyväksikäyttämiseen. Hyökkäyksessä käytettyjä viestejä voi olla vaikeata erottaa normaalista CAN-väylän liikenteestä, ja monet jo olemassa olevat järjestelmät epäilyttävien viestien havaitsemiseksi eivät välttämättä havaitisi mitään epätavallista, koska käytetyt viestit vaikuttaisivat väylässä kulkevilta virheviesteiltä, joka vaikuttaisi normaalilta (Cho & Shin, 2016).

3.2 Epäsuorat hyökkäykset

Suoraan fyysisesti toteutetut hyökkäykset autojen sisäisiä tietoverkkoja vastaan on havaittu erittäin tehokkaiksi, ja niiden potentiaali aiheuttaa haittaa tai vaaratilanteita korkeaksi (Koscher et al., 2010). Kuitenkin näitä tuloksia on kritisoitu perustuen siihen, että oletus hyökkääjän kyky olla suoraan fyysisesti yhteydessä autoon on epärealistinen suuressa osassa tapauksia (Checkoway, McCoy, Kantor, Anderson, Shacham, Savage, Koscher, Czeskis, Roesner & Kohno, 2011).

Vaihtoehtona fyysisille hyökkäyksille ovat epäsuorat hyökäykset, jotka pystytään toteuttamaan ilman, että hyökkääjän tarvitsee välttämättä olla hirveän lähellä autoa. Tämän kaltaisia epäsuoria haavoittuvuuksia on löydetty esimerkiksi autojen PKES (Passive Keyless Entry and Start)-järjestelmistä (Francillon, Danev & Capkun, 2011; Alrabady & Mahmud, 2005). PKES-järjestelmät mahdollistavat auton ovien lukkojen avaamisen ja moottorin käynnistämisen ilman fyysistä avainta, niin kauan kun käyttäjällä on mukanaan avaimenperä, jonka lähettämän langattoman signaalin auton järjestelmät vastaanottavat ja hyväksyvät (Francillon et al., 2011; Alrabady & Mahmud, 2005). Francillon et al. (2011) suorittamassa testissä huomattiin, että tarkastellut PKES-järjestelmät olivat haavoittuvaisia relehyökkäykselle, joka oli toteutukseltaan hyvin samanlainen kuin ”kahden varkaan metodi”, jonka Alrabady et al. (2005) olivat tutkimuksessaan esittäneet. Hyökkäyksen idea perustui kannettaviin sensoreihin, joista ensimmäistä pidettiin lähellä auton ovea, ja toista lähellä PKES avaimenperää (Francillon et al., 2011). Auton lähettämä signaali toistettiin langattomasti PKES avaimenperälle, jonka lähettämä vastausignaali taas toistettiin langattomasti takaisin autolle, joka kuittasi tunnistuksen hyväksytyksi, avaten oven lukot (Francillon et al., 2011). Francillon et al. (2011) suorittamassa testissä tämä relehyökkäys todettiin toimivaksi kaikissa kymmenessä autossa, joita vastaan sitä testattiin.

Tutkimuksessaan Francillon et al. (2011) esittää myös erilaisia keinoja, joilla estää kuvatuunkaltaisen relehyökkäyksen toteuttaminen autoa vastaan. Välittömiä, käyttäjän toetuttamia ratkaisuja ovat esimerkiksi avaimenperän pitäminen metallisessa säilytysrasiassa kun sitä ei tarvita, jolloin avaimenperän signaalin lukeminen ja

välittäminen eteenpäin vaikeutuvat huomattavasti (Francillon et al., 2011). Toisena mahdollisuutena esitettiin jo paikoittain käytössä olevaa tapaa, jossa auto mittaa saamansa signaalin vahvuuden, ja tämän pohjalta yrittää laskea, kuinka kaukana signaalin lähettäjä on (Francillon et al., 2011). Kuitenkin nämä ovat parhaimmillaan väliaikaisia ratkaisuja, tai jälkimmäisen tapauksessa helposti kierrettävissä. Realistisimpana vaihtoehtona esitettiin distance bounding protokollan implementoimista, jonka avulla voidaan varmistaa, että auto ja sen lähetämään signaliin vastannut kohde ovat tietyn matkan päässä toisistaan ja tällä tavalla estää avaimen signaalin lukeminen etänä (Francillon et al., 2011; Yang, Kong, Xin, Hu, & Chen, 2012).

Myös muut auton CAN-verkon ja sen ulkopuolisen maailman kanssa langattomasti yhteydessä olevat teknologiat ja protokollat voivat olla mahdollinen vektori hyökkäykselle. Tutkimuksessaan esimerkiksi Lang, Dittmann, Kiltz ja Hoppe (2007) käyvät läpi mahdollisia haavoittuvuuksia, joita internettiin yhdistetty auto ja sen IP-osoite saattaisivat sisältää. Tarvetta tämän kaltaiselle teknologialle autoissa tulee tulevaisuudessa todennäköisesti olemaan, ottaen huomioon elektroniikan määrän kasvun ajoneuvoissa, sekä tämän pohjalta muodostuvan tarpeen päivittää laitteiden ajureita ja ohjelmistoja nopeasti ja tehokkaasti langattomalla yhteydellä (Lang et al., 2007). Jos nämä teknologiat implementoidaan ajoneuvoihin tulevaisuudessa, tulevat ne olemaan alttiita samankaltaisille hyökkäyksille, jotka ovat nykyään uhkana myös tietokoneille, kuten MITM (Man in the middle) -hyökkäykset, joissa hyökkääjä sieppaa kahden kohteen välillä kulkevaa viestivirtaa, ja tekee siihen omia muokkauksia ennen kuin lähettää sen eteenpäin (Lang et al., 2007). Vaikkakin langattoman viestinnän teknologiat eivät suoraan liity auton sisäisen CAN-verkon tietoturvaluuteen, on erilaisia hyökkäysmetodeja hyödyntämällä mahdollista murtautua sisään auton CAN-verkkoon yhdistettyyn laitteeseen, ja tätä kautta vakoilla auton sisäistä kommunikaatiota tai muuten yrittää vaikuttaa sen toimintaan esimerkiksi lähettämällä väärennettyjä CAN-viestejä.

Toinen esimerkki protokollaan pohjautuvasta heikkoudesta on vastikään Vanhoefin (2017) esille nostama heikkous WPA:ssa ja WPA2:ssa, jotka ovat Wi-Fi-verkoissa käytettyjä turvallisuusprotokollia. Havaittu heikkous on protokollissa käytetyssä nelisuuntaisessa kädenpuristuksessa (4-way handshake): normaalisti tätä suoritettaessa käytetään avaimina kertakäyttöisiä lukuja autentikaatiossa, joita ei tulisi käyttää enää uudelleen (Vanhoef, 2017). Kuitenkin protokollassa on olemassa heikkous, jota hyväksikäyttämällä hyökkääjä pystyy saamaan kohteen uudelleenkäyttämään tällaisen avaimen, jos hän seuraa liikennettä ja lähettää uudelleen tiettyjä paketteja kohteelle (Vanhoef, 2017). Huonoimmista tapauksista oli tämän avulla mahdollista purkaa salaus lähetetyistä viesteistä ja lukea niiden sisältöä, joka vaarantaa niiden luottamuksellisuuden (Vanhoef, 2017). Ottaen huomioon Lang et al. (2007) aikaisemmin mainitsemat ongelmat autojen mahdollisen IP-protokollan hyödyntämisessä tulevaisuudessa, myös tätä WPA/WPA2 haavoittuvuutta, tai sen kaltaisia haavoittuvuuksia, voitaisiin käyttää hyväksi CAN-verkon laitteiden tietoturvan murtamisessa ulkoa käsin, jos kyseessä olevat laitteet hyödyntävät WPA-protokollaa viestinnässään esimerkiksi päivityksiä ladatessaan.

4. Tietoturvan parantaminen

Muutamissa aikaisemmin mainituissa hyökkäystekniikoissa (Alrabady & Mahmud, 2005; Hoppe et al., 2008; Francillon et al., 2011; Yang et al., 2012) on myös samalla käyty läpi potentiaalisia puolustuskeinoja, joita voitaisiin käyttää estämään niiden kaltaiset hyökkäykset tulevaisuudessa, tai ainakin jollain tavalla vähentämään niistä aiheutuvia riskejä ja vaaroja. Nämä olivat kuitenkin suurelta osin vain alalukuja tutkimuksissa, joiden tarkoituksena oli löytää ja käyttää hyväksi auton sisäisen verkon tietoturva-aukkoja. Seuraavassa luvussa käyään tarkemmin läpi tutkimuksia, jotka keskittyvät enemmän näiden tietoturvaongelmien korjaamiseen joko esittämällä kokonaan uusia tekniikoita joita voitaisiin soveltaa, tai auttavia järjestelmiä, jotka voitaisiin liittää osaksi olemassa olevia.

4.1 Komponenttien kryptografinen varmennus

Suurena ongelmana autojen sisäisten tietoverkkojen tietoturvassa on siihen liitettyjen komponenttien autentikointi, joka on erityisesti CAN-verkon tapauksessa erittäin vaikeaa johtuen sen suunnitteluperiaatteista. Yhtenä keinona esimerkiksi väärennetyjä tai muuten tarkoituksella ilkeämielisesti tuotettuja komponentteja vastaan on ehdotettu osien kryptografista merkitsemistä. Weimerskirch et al. (2005) ehdottamassa tekniikassa olisi keskeisessä roolissa autoon asennettu laitteiston turvamoduuli (engl. Hardware Security Module, HRM), jonka avulla tunnistettaisiin kaikki autoon asennettavat osat asymmetrisen kryptografian avulla. Weimerskirch et al. (2005) mukaan komponentin elinkaareissa olisi tällöin kolme eri vaihetta: autentikointi asennusvaiheessa, käytön aikana ja silloin, kun osa lopulta poistetaan autosta. Sen lisäksi, että komponenteissa olisi avainten- ja viestienvaihdon mahdollistava RFID transponderi, vaadittaisiin lisäksi myös se, että validit varaosat pystyisivät esittämään järjestelmälle sertifikaatin, joka todistaisi niiden olevan aitoja, eikä väärennöksiä (Weimerskirch et al., 2005).

Weimerskirch et al. (2005) esittämässä tavassa uutta komponenttia autoon asennettaessa sisäinen turvamoduuli varmistaisi komponenteilta niiden sertifikaatit, ja jos nämä olisivat kunnossa, järjestelmä lähettäisi niille tunnistautumisavaimen, jonka avulla ne tulevaisuudessa pystyisivät tunnistautumaan aidoiksi. Kryptografisen avaimen perustuva autentikointi suoritettaisiin aina auton käynnistämisen yhteydessä, ja sellaisissa tapauksissa, joissa osa ei kykene tunnistautumaan hyväksyttävästi, auto ei käynnistyisi tai antaisi ajajalle virheilmoituksen, riippuen ongelman vakavuudesta. Kun autosta poistetaan komponentteja, autentikointia käytettäisiin varmentamaan se, että osa poistetaan oikein, eikä sitä olla esimerkiksi varastamassa (Weimerskirch et al., 2005).

Komponenttien kryptografista varmennusta käytettäessä on kuitenkin otettava huomioon, että jos autentikointitiliosiosissa luotetaan pelkästään auton oman turvamoduulin avulla saatuun tulokseen, ei välttämättä pystytä suojautumaan siltä, että ulkopuolinen toimija suoraan kloonaisi jonkin auton osan, eli tuottaisi siitä tarpeeksi tarkan kopion, joka sisältää myös autentikoinnissa käytetyt avaimet. Jos mahdollistetaan se, että turvamoduuli pystyy ottamaan yhteyttä ulkoiseen järjestelmään ja tätä kautta varmentamaan käytetyt avaimet tätä kautta, kloonaminen vaikeutuisi (Weimerskirch et al., 2005).

Vaikkakin komponenttien kryptografista varmennusta käyttämällä pystyttäisiin tehokkaasti estämään auktorisoimattomien osien päätyminen autoon, tulisi se kuitenkin tiukasti rajoittamaan niitä tahoja, jotka saavat ja pystyvät tuottamaan niin sanotusti ”aitoja” osia. Lisäksi on huomioitava myös se, että pelkällä sisäisellä autentikoinnilla ongelmia voi silti aiheutua väärennetyistä osista, jotka ovat tarpeeksi samanlaisia luikahtaakseen autentikointijärjestelmän seulan läpi (Weimerskirch et al., 2005).

Edellä mainittuja tekniikoita ja parannuksia niihin on tarkasteltu myöhemmässä kirjallisuudessa. Tällaisia ovat olleet esimerkiksi tutkimukset fyysisesti kloonaamattomien funktioiden (Physically Unclonable Function, PUF) hyödyntämisestä kryptografisessa varmennuksessa ja turvallisessa kommunikaatiossa, sekä myös mahdollisena toteutustekniikkana Weimerskirch et al. (2005) esittämiin varkaudenestojärjestelmiin (Asim, Guajardo, Kumar & Tuyls, 2009). Idea perustuu Pappun, Rehtin, Taylorin ja Gershenfeldin (2002) kehittämään tekniikkaan käyttää fyysisen materiaalin satunnaista rakennetta tuottamaan samankaltaisia tuloksia kuin matemaattiset yksisuuntaiset kryptografiset funktiot.

Jatkeena tai vaihtoehtona fyysisesti kloonaamattomille funktioille on myöhemmin esitetty myös salaisten tuntemattomien salakoodien (Secret Unknown Cipher, SUC) käyttöä mikrokontrollereissa (Mars & Adi, 2018). Tekniikassa osien valmistusvaiheessa mikrokontrolleriin injektoidisiin ohjelmisto, joka satunnaislukugeneraattorin avulla laskisi avaimen, joka olisi jokaisen mikrokontrollerin tapauksessa sille uniikki ja ainoastaan sen itsensä tiedossa. Tämän jälkeen avaimen laskentaan käytetty ohjelmisto poistettaisiin, ja mikrokontrollerien tuntemattomia avaimia käytettäisiin autentikoimaan muut väylässä olevat osat (Mars & Adi, 2018).

4.2 Epätavallisten CAN-viestien tunnistaminen ja/tai suodattaminen

Johtuen siitä, että CAN-viestit eivät sisällä tietoa lähettäjistä ja vastaanottajasta, voi olla vaikeaa tunnistaa oikeat viestit väärennetyistä. Tämän takia tutkimuksessa on keskitytty enemmän siihen, että mahdollisesti väärennetyt CAN-viestit pystytään havaitsemaan muiden keinojen, kuten viestiliikenteen analyysin tai tunnistusalgoritmien avulla (Marchetti & Stabili, 2017; Ling & Feng, 2012). Viestiliikenteen analyysissä tarkasteltiin CAN-väylässä liikkuvien viestien frekvenssiä, jota vuorostaan käytettiin pohjana tunkeutumisen havaitsemisjärjestelmän kehittämisessä (Song, Kim & Kim, 2016).

Edellä mainitut ovat spesifejä sovellusalueita, joita voitaisiin käyttää yhtenä osana auton sisäisen verkon palomuurijärjestelmää. Tällaisen järjestelmän integroimista elektronisten kontrolloyksiköiden ja CAN-verkon väliin on ehdotettu, ja se toimisi samantyyppisellä periaatteella kuin perinteinen palomuri tietokoneissa, tarkastaen saapuvia CAN-paketteja ja suodattamalla tai estämällä sellaisten pakettien saapumisen, jotka vaikuttavat epäilyttäviltä (Pan, Zheng, Chen, Luan, Bootwala & Batten, 2017).

Song et al. (2016) suorittamassa CAN-väylän viestiliikenteen analyysissä vertailtiin väylässä kulkevien viestien välistä frekvenssiä normaalissa tilanteessa, sekä lisäksi silloin, kun järjestelmää vastaan simuloitiin injektiohyökkäystä. Johtuen väärennetyjen CAN-viestien välisen aikafrekvenssin pienuudesta verrattuna valideihin viesteihin, tutkimuksessa huomattiin selvä ero, jonka avulla viestityypit pystyttiin erottamaan toisistaan (Song et al., 2016). Monella tapaa tämä vastaa Hoppe et al. (2008) aikaisemmin ehdottamaa tapaa, jolla väärennetyt CAN-viestit pystyttäisiin mahdollisesti tunnistamaan väylässä.

Vaikkakin esitetty tekniikka on toteutukseltaan hyvin yksinkertainen ja perustuu suurelta osin huomioon, jota voidaan pitää itsestäänselvänä, on se kuitenkin käyttökelpoinen suojaamaan CAN-väylää hyökkäystyypeiltä, joissa injektoidaan suuri määrä viestejä järjestelmään siinä toivossa, että niiden määrä aiheuttaa tukoksen ja estää valideja viestejä pääsemästä perille (Song et al., 2016).

Marchettin ja Stablin (2017) esittämä algoritmi epätavallisten ja mahdollisesti väärennetyjen CAN-viestien tunnistamiseen taas perustuu tekniikkaan, jossa auton validien CAN-viestien pohjalta muodostetaan kuva siitä, millaisia hyväksyttäviä viestejä järjestelmässä kulkee. Aluksi muodostetaan matriisi hyväksyttävistä viestikoodeista, jonka kaikki arvot on oletuksena asetettu epätodeksi (Marchetti & Stabili, 2017). Kun tämä myöhemmin yhdistetään matriisiin, joka sisältää validista CAN-viestittelysessiosta saatuja viestejä, lopputuloksena on matriisi, jossa validit viestit saavat arvon tosi, ja potentiaalisesti väärät, joita viestivirrassa ei havaittu, saavat arvon epätosi (Marchetti & Stabili, 2017).

Kuvattua menetelmää pystytään siis käyttämään auton sisäisen CAN-verkon liikenteen analysointiin siten, että auton CAN-verkon normaalin liikenteen pohjalta muodostettua matriisia käytetään verkossa kulkevien viestien tunnistamiseen (Marchetti & Stabili, 2017).

Näiden analyysi- ja tunnistustekniikoiden lisäksi on esitetty myös CAN-väylään kytkettyjen elektronisten kontrolliyksiköiden tunnistamista perustuen itse signaaleissa oleviin eroihin, joiden avulla on mahdollista laskea omat uniikit tunnisteet väylään kytketyille kontrolliyksiköille (Avatefipour, Hafeez, Tayyab & Malik, 2017; Choi, Jo, Woo, Chun, Park & Lee, 2018; Groza & Murvay 2018).

Choi et al. (2018) esittämä, Avatefipour et al. (2017) aikaisempaan tutkimukseen perustuvassa metodissa väylään kytketään ylimääräinen kontrolliyksikkö, joka koulutetaan valvotusti tunnistamaan muiden väylään kytkettyjen kontrolliyksiköiden signaalit ja näiden pohjalta muodostamaan tunnisteet hyväksytyistä järjestelmään kytketyistä laitteista. Koska Choi et al. (2018) esittämä tunnistustekniikka perustuu ulkoiseen tarkkailuun, sen implementoiminen ei varsinaisesti vaadi muuta kuin ylimääräisen kontrolliyksikön asentamisen ja kalibroimisen. Kontrolliyksiköiden laitekoodin päivittäminen saattaa myös olla tarpeellista, sillä esitetty metodi hyödyntää pidennettyä CAN-kehysten pidennettyä formaattia normaalin lyhyemmän sijaan parantaakseen tunnistustarkkuutta, eivätkä kaikki mikrokontrollerit automaattisesti tue tätä (Choi et al., 2018). Huomionarvoista on lisäksi myös sinällään se, että kokeessa kuvailtu asetelma ei pysty hyvin ottamaan huomioon tilannetta, jossa hyökkääjä on onnistunut lisäämään oman kontrolliyksikkönsä väylään, tai saanut jonkin jo kytketyistä vallattua ennen valvovan kontrolliyksikön opetusvaihetta (Choi, 2018).

5. Pohdinta

Tässä tutkielmassa tarkasteltiin autojen sisäisten CAN-verkkojen tietoturvaluutta pääasiallisena tutkimuskysymyksenä: millaisia ympäristöjä CAN-verkot ovat tietoturvan suhteen, ja onko niissä arkkitehtuurista tai väärinkäytöksistä johtuvia ongelmia, jotka vaarantavat turvallisuuden? Tämän lisäksi pyrittiin käsittelemään myös mahdollisia ratkaisuja näihin tietoturvaongelmiin. Elektroniikan ja erinäisten langattomien laitteiden määrän lisääntyminen autoissa vuosien saatossa on johtanut moniin erilaisiin muutoksiin ja innovaatioihin, jotka ovat luonteeltaan olleet sekä hyödyllisiä, auton toimintaa tehostavia, että myös tuoneet monia luksusominaisuuksia niihin (Cook et al., 2007, Bosch, 2014). Kuitenkin monessa määrin autojen tietoturva näiden sisäisten järjestelmien suhteen on jäänyt jälkeen, kun sitä verrataan autojen muihin ominaisuuksiin turvallisuuden saralla, kuten kolaritilanteissa joissa käyttäjää suojelemaan on kehitetty vuosien saatossa esimerkiksi turvavyöt, airbagjärjestelmät sekä kolaritilanteissa turvallisesti rikkoutuvat korin rakenteet (Wolf, Weimerskirch & Wollinger, 2007; Larson & Nilsson, 2008; Islam, Lautenbach, Sandberg & Olovsson, 2016).

Suuri osa autojen CAN-verkkojen ongelmista juontuvat itse protokollan luonteesta, sekä tavasta millä näiden verkkojen topologia autoissa toimii (Carsten et al., 2015). Siispä ellei tulevaisuudessa kehitetä kokonaan uudenlaista väyläjärjestelmää korvaamaan CAN:ia tai muita vastaavia toteutuksia, joutuvat sen ongelmia ratkovat paljolti keskittymään ratkaisuihin, jotka asettuvat CAN-verkon ja sen avulla kommunikoidvien laitteiden väliin. Palomuurien (Pan et al., 2017), viestien tunnistus- (Song et al., 2016) ja seulonta-algoritmien (Marchetti & Stabili, 2017) sekä osien kryptografisen varmennuksen (Weimerskirch et al., 2005) avulla saavutetut korjaukset ovat suurelta osin toimivia ratkaisuja, ainakin väliaikaisesti kunnes hyökkääjät ja rikolliset toimijat muuttavat toimintatapojaan kiertääkseen näitä turvakeinoja.

Kaiken kaikkiaan tarkastellun kirjallisuuden pohjalta voitaisiin yleisesti arvioida, että autojen tietoturva on käymässä läpi murrosta. Autoissa olevan elektroniikan määrä tuskin tulee ainakaan laskemaan tulevien vuosien ja vuosikymmenien aikana, ja on hyvin todennäköistä, että sekä sähkö- että itseajavien autojen kehittyminen tänä aikana tulee ajamaan tätä kehitystä kasvavaan suuntaan. Myös IoT-laitteiden määrän kasvu nykyaikana tulee todennäköisesti lisäämään tätä sekä tarvetta liittää langatonta teknologiaa autoihin tuomaan lisää toiminnallisuutta, kuten mahdollisuuden päivittää käytettyjä ohjelmistoja tai ajureita etänä. Internet yhteyden tuominen autoihin tulee tuomaan jälleen uuden hyökkäyspinnan niihin (Lang et al., 2007), joka altistaa ne samankaltaisille ongelmille kuin modernit, internetyhteydellä varustetut tietokoneetkin.

Vuosien saatossa autot ovat vakiinnuttaneet itsensä osaksi ihmisten elämää, ja verrattuna 1900-luvun alun tilastoihin, niiden lukumäärä on vuosisadassa kasvanut valtavasti (Cook et al., 2007), ja niistä on suurelle osalle tullut itsestänselvyys. Kuitenkin tässä tutkielmassa tarkastellun kirjallisuuden pohjalta vaikuttaa siltä, että ajoneuvoissa piilee monia nopean modernisaation mukanaan tuomia tietoturvaongelmia, jotka altistavat ne vaaratilanteille. Nämä ongelmat eivät ole aina välttämättä myöskään sellaisia, joiden olemassaolon tavallinen ihminen pystyisi silmämääräisesti autostaan toteamaan. Tämän takia olisikin hyvä, jos teollisuus alkaisi todella panostaa ajoneuvojen tietoturvaan, sillä sähkö- ja itseajavien autojen yleistyessä nämä ongelmat tuskin tulevat ainakaan vähenemään.

6. Yhteenveto

Tämän työn tarkoituksena oli kirjallisuuskatsauksen avulla tarkastella ja analysoida autojen CAN-verkkojen tietoturvan tasoa, siihen liittyviä ongelmakohtia, sekä myös potentiaalisia ratkaisuja näihin ongelmiin. Huomionarvoista oli se, kuinka laaja konsensus liittyen CAN-väylän tietoturvattomuuteen oli. Paljolti tämä juonsi syynsä väyläprotokollan itsensä perusteisiin (Lawrenz, 2013; Bosch, 2014), joiden takia se oli luonnostaan erittäin altis erilaisille hyökkäyksille.

Itse CAN-väylän tietoturva-aukkojen hyödyntämisestä on vuosien saatossa tehty paljon tutkimusta, joka on luonteeltaan ollut hyvin vaihtelevaa. Sekä puhtaasti teoreettisia tutkimuksia, että myös käytännönläheisempiä kokeita autoille kenttäolosuhteissa on suoritettu (Koscher et al., 2010; Francillon et al., 2011). Tässä kirjallisuuskatsauksessa tarkasteltiin kahta erilaista lähestymistapaa, jotka olivat etä- ja fyysiset hyökkäykset. Tarkastelluissa tutkimuksissa, joissa yritettiin esimerkiksi auton OBD-II portin tai muiden fyysisten reittien kautta päästä käsiksi väylään, tulokset olivat lähes poikkeuksetta onnistumisia: väärin CAN-viestien lähettäminen oli helppoa, ja löydettiin myös tapauksia, joissa väylään yhdistetyt auton komponentit saatiin tekemään asioita, joita niiden ei valmistajien mukaan tulisi turvallisuussyistä pystyä tekemään (Koscher et al., 2010). Tällaisia olivat esimerkiksi elektronisten kontrolliyksiköiden muistien pyyhkiminen, ja niiden CAN-kommunikation sulkeminen kokonaan (Koscher et al., 2010). Myös etänä suoritettavat hyökkäykset olivat onnistuneita, kuten auton automaattisen lukituksen purkamisen relehyökkäyksen avulla, joka kohdistettiin tätä järjestelmää langattomasti kontrolloivaan PKES-avaimenperään (Francillon et al., 2011).

Parannusehdotukset CAN-väylän tietoturvaan keskittyivät paljolti lisäyksiin, jotka tehostaisivat siinä olevien laitteiden kykyä tunnistaa vahingollisia CAN-viestejä tai liikennettä (Ling & Feng, 2012, Marchetti & Stabili, 2017). Tällaisia olivat esimerkiksi auton sisäisen palomuurin osana toimivat tunnistusalgoritmit, jotka pystyisivät havaitsemaan epätavalliset viestit (Marchetti & Stabili, 2017), tai yksinkertaisimmillaan CAN-väylän viestiliikenteen frekvenssianalyysi, jonka avulla oli mahdollista tunnistaa normaalit viestit mahdollisesti väärennetyistä (Song et al., 2016). Näiden lisäksi myös auton osien kryptografista varmennusta esitettiin keinona vähentää tarkoituksella väärennetyistä osista koituvaa uhkaa (Weimerskirch et al., 2005).

Suurimmassa osassa tutkimuksia joissa tarkasteltiin olemassa olevissa autoissa olevia CAN-verkon tietoturvaongelmia, testattavia ajoneuvoja oli vain muutama kappale testeissä (Koscher et al., 2010; Francillon et al., 2011). Tulevan tutkimuksen kannalta olisikin hyvä, jos laajamittaisempia ja systemaattisempia testejä saataisiin suoritettua suuremmalle määrälle ajoneuvoja mahdollisimman monilta eri valmistajilta. Näin saadun tiedon pohjalta pystyttäisiin kokoamaan laajempia tilastoja siitä, millaisia tietoturvapuutteita autoista noin yleensä löytyy, sekä myös ovatko jotkin ongelmat valmistajakohtaisia.

7. Lähdeluettelo

- Alrabady, A. I., & Mahmud, S. M. (2005). Analysis of Attacks Against the Security of Keyless-Entry Systems for Vehicles and Suggestions for Improved Designs. *IEEE Transactions on Vehicular Technology*, 54(1), 41-50.
- Asim, M., Guajardo, J., Kumar, S. S., & Tuyls, P. (2009). Physical Unclonable Functions and Their Applications to Vehicle System Security. *VTC Spring 2009-IEEE 69th Vehicular Technology Conference*, 1-5.
- Avatefipour, O., Hafeez, A., Tayyab, M., & Malik, H. (2017). Linking Received Packet to the Transmitter Through Physical-Fingerprinting of Controller Area Network. *2017 IEEE Workshop on Information Forensics and Security (WIFS)*, 1-6.
- Bosch, R. (2014). Bosch Automotive Electrics and Automotive Electronics: Systems and Components, Networking and Hybrid Drive (5th ed.). In Robert Bosch GmbH (Ed.), *Bus Systems*, 92-150. Plochingen, Germany
- Bozdal, M., Samie, M., & Jennions, I. (2018). A Survey on CAN Bus Protocol: Attacks, Challenges, and Potential Solutions. *2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE)*, 201-205.
- Buttigieg, R., Farrugia, M., & Meli, C. (2017). Security Issues in Controller Area Networks in Automobiles. *2017 18th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)*, 93-98.
- Carsten, P., Andel, T. R., Yampolskiy, M., & McDonald, J. T. (2015). In-Vehicle Networks: Attacks, Vulnerabilities, and Proposed Solutions. *Proceedings of the 10th Annual Cyber and Information Security Research Conference*.

- 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. *USENIX Security Symposium*, volume 4, 447-462.
- Cho, K. T., & Shin, K. G. (2016). Error Handling of In-Vehicle Networks Makes Them Vulnerable. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 1044-1055.
- Choi, W., Jo, H. J., Woo, S., Chun, J. Y., Park, J., & Lee, D. H. (2018). Identifying ECUs Using Inimitable Characteristics of Signals in Controller Area Networks. *IEEE Transactions on Vehicular Technology*, 67(6), 4757-4770.
- Cook, J. A., Kolmanovsky, I. V., McNamara, D., Nelson, E. C., & Prasad, K. V. (2007). Control, Computing and Communications: Technologies for the Twenty-First Century Model T. *Proceedings of the IEEE*, 95(2), 334-355.
- Francillon, A., Danev, B., & Capkun, S. (2011). Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars. *Proceedings of the Network and Distributed System Security Symposium (NDSS)*. Eidgenössische Technische Hochschule Zürich, Department of Computer Science.
- Groza, B., & Murvay, P. S. (2018). Security Solutions for the Controller Area Network: Bringing Authentication to In-Vehicle Networks. *IEEE Vehicular Technology Magazine*, 13(1), 40-47.
- Hoppe, T., Kiltz, S., & Dittmann, J. (2008). Security Threats to Automotive CAN Networks—Practical Examples and Selected Short-Term Countermeasures. *International Conference on Computer Safety, Reliability, and Security*, 235-248.

- Islam, M. M., Lautenbach, A., Sandberg, C., & Olovsson, T. (2016). A Risk Assessment Framework for Automotive Embedded Systems. *Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security*, 3-14.
- Kleberger, P., Olovsson, T., & Jonsson, E. (2011). Security Aspects of the In-vehicle Network in the Connected Car. *Intelligent Vehicles Symposium (IV)*, 2011 IEEE, 528-533.
- Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H. & Savage, S., (2010). Experimental Security Analysis of a Modern Automobile. *2010 IEEE Symposium on Security and Privacy*, 447-462.
- Koushanfar, F., Sadeghi, A., & Seudie, H. (2012). EDA for Secure and Dependable Cybercars: Challenges and Opportunities. *Proceedings of the 49th Annual Design Automation Conference*, 220-228.
- Lang, A., Dittmann, J., Kiltz, S., & Hoppe, T. (2007). Future Perspectives: The car and Its IP-address—a Potential Safety and Security Risk Assessment. *International Conference on Computer Safety, Reliability and Security*, 40-53.
- Larson, U. E., & Nilsson, D. K. (2008). Securing Vehicles Against Cyber Attacks. *Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research: Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead*, 30.
- Lawrenz, W. (2013). CAN Basic Architectures, 1-40. In: Lawrenz W. (Eds.) *CAN System Engineering: From Theory to Practical Applications* (2nd ed). Springer, London

- Ling, C., & Feng, D. (2012). An Algorithm for Detection of Malicious Messages on CAN Buses. *Proceedings of the 2012 National Conference on Information Technology and Computer Science (CITCS)*, 2012.
- Marchetti, M., & Stabili, D. (2017). Anomaly Detection of CAN Bus Messages Through Analysis of ID Sequences. *2017 IEEE Intelligent Vehicles Symposium (IV)*, 1577-1583.
- Mars, A., & Adi, W. (2018). Clone-Resistant Entities for Vehicular Security. *2018 International Conference on Innovations in Information Technology (IIT)*, 18-23.
- Othmane L.B., Weffers H., Mohamad M.M., Wolf M. (2015) A Survey of Security and Privacy in Connected Vehicles. In: Benhaddou D., Al-Fuqaha A. (eds) *Wireless Sensor and Mobile Ad-Hoc Networks*. 217-247. Springer, New York, NY
- Pan, L., Zheng, X., Chen, H. X., Luan, T., Bootwala, H., & Batten, L. (2017). Cyber Security Attacks to Modern Vehicular Systems. *Journal of Information Security and Applications*, 36, 90-100.
- Pappu, R., Recht, B., Taylor, J., & Gershenfeld, N. (2002). Physical One-Way Functions. *Science*, 297(5589), 2026-2030.
- Song, H. M., Kim, H. R., & Kim, H. K. (2016). Intrusion Detection System Based on the Analysis of Time Intervals of CAN Messages for In-Vehicle Network. *International Conference on Information Networking*, 63-68.
- Takahashi, J., Tanaka, M., Fuji, H., Narita, T., Matsumoto, S., & Sato, H. (2018). Abnormal vehicle behavior induced using only fabricated informative CAN messages. *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 134-137.

- Vanhoef, M., & Piessens, F. (2017). Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 1313-1328.
- Weimerskirch, A., Paar, C., & Wolf, M. (2005). Cryptographic Component Identification: Enabler for Secure Vehicles. *IEEE Vehicular Technology Conference*, 62(2), 1227.
- Whitman, M. E. & Mattord, H. J. (2011). *Principles of Information Security* (4. ed.). Introduction to Information Security, 1-42. Australia: Course Technology/Cengage Learning.
- Wolf, M., Weimerskirch, A., & Wollinger, T. (2007). State of the Art: Embedding Security in Vehicles. *EURASIP Journal on Embedded Systems*, 2007(1), 1-16.
- Yang, T., Kong, L., Xin, W., Hu, J., & Chen, Z. (2012). Resisting Relay Attacks on Vehicular Passive Keyless Entry and Start Systems. *2012 9th International Conference on Fuzzy Systems and Knowledge Discovery*, 2232-2236.