Janne Tervo

Ajoneuvoteknisten järjestelmien tietoturvallisuusselvitys

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Ajoneuvotekniikka

Insinöörityö

25.5.2018

Metropolia

Tekijä Otsikko Sivumäärä Aika	Janne Tervo Ajoneuvoteknisten järjestelmien tietoturvallisuusselvitys 57 sivua 25.5.2018
Tutkinto	Insinööri (AMK)
Tutkinto-ohjelma	Ajoneuvotekniikka
Ammatillinen pääaine	Autosähkötekniikka
Ohjaajat	Lehtori Pasi Kovanen

Tämän insinöörityön tavoitteena oli selvittää ajoneuvoteknisten järjestelmien tietoturvallisuutta Metropolia Ammattikorkeakoululle. Työssä käsitellään ajoneuvojen tietoturvallisuudesta laadittuja väitöskirjoja, ajoneuvoteknisen tietojärjestelmän murtautumistapausta, tietoturvallisuus- sekä ajoneuvoteknisiä standardeja, tietojärjestelmien perusrakennetta ja tietoturvallisuuden yleisimpiä käytäntöjä.

Työn tavoitteena on tuottaa suomenkielistä materiaalia aiheesta. Työssä tarkastellaan ajoneuvojen tietoturvallisuuden perustaa, verkottumisen vaikutuksia tietoturvallisuuteen sekä menetelmiä riskien minimointiin. Johdannon ja tavoitteiden jälkeen käsitellään tietojärjestelmän yleistä rakennetta, tietoturvallisuuden erilaisia suojausjärjestelmiä sekä näihin liittyviä standardeja ja terminologiaa. Seuraavaksi siirrytään varsinaisiin ajoneuvoihin liittyviin tietoturvallisuusaspekteihin, kartoitetaan ajoneuvoihin liittyviä tietoturvallisuusuhkia ja esitellään samalla autovarkauksia sekä esimerkkitapaus. Sen jälkeen esitellään ajoneuvojen suojatumista tietoturvallisuusuhkilta.

Ajoneuvojen tietoturvallisuudelle ei ole käytännössä mitään pätevää standardisointia. Lisäksi ajoneuvojen sähköistyminen on lisännyt ajoneuvojen haavoittuvuutta erilaisille tietohyökkäyksille. Jopa ajoneuvon haltuunotto langattoman verkon kautta on teoriassa täysin mahdollista, käytännössä siihen kuitenkin vaaditaan taloudellisia resursseja ja erityisen hyvää tuntemusta ajoneuvojen tietojärjestelmien rakenteesta ja ohjelmoinnista. Erilaiset haavoittuvuudet ajoneuvoissa luovat osaavalle rikolliselle laajan skaalan eri liiketoiminnan malleja.

Insinöörityön lopputuloksena syntyi kokonaisvaltainen kuva ajoneuvoteollisuuden tietoturvallisuuden tärkeydestä, sen osittain heikosta tilasta ja tavoista sen kehittämiseen.

Avainsanat	ajoneuvo, tietoturvallisuus, auton hakkerointi

Author	Janne Tervo
Title	Study of Information Security in Vehicular Technical Systems
Number of Pages	57 pages
Date	25 August 2017
Degree	Bachelor of Engineering
Degree Programme	Automotive Engineering
Professional Major	Automotive Electronics Engineering
Instructors	Pasi Kovanen, Senior Lecturer

The aim of this Bachelor's thesis was to clarify the information security of vehicular technical systems for Metropolia University of Applied Sciences. In this study dissertations regarding information security in the automotive domain are reviewed. Also, an exemplary study case of hacking an information system of a passenger vehicle was viewed. In addition, this study explains the general structure of an information system and the means of conduct in the field of information security.

The objective of this thesis is to create written material in Finnish on the subject. First the thesis clarifies the structure of an information system and the means of protecting that system. This includes terminology and standardization of information systems and security. Next, the thesis moves on to the actual vehicular side of information security. Threats in this area are analyzed and the case study with some grand theft auto data are reviewed. Then the thesis proceeds to the means of protecting an information system from hackers in the automotive domain.

The standardization of information security in vehicular applications is in fact, quite inadequate. The electrification of automotive components has increased the vulnerability of automobiles to different sorts of attacks. Even taking control of a vehicle has become possible in theory. However, in practice this requires some financial resources and a very broad skillset on coding and knowledge of the information system structure in vehicles and so forth. Different sorts of vulnerabilities have provided the skillful criminal with a wide scale of business models.

In this study, comprehensive pictures of the importance of information security, the partial lack of it and the means of improvement in vehicles were formed.

Keywords	Vehicle, information security, car hacking

Sisällys

Lyhenteet

ADAC	Allgemeiner Deutscher Automobil-Club. Saksalainen autokerho.
AES	Advanced Encryption Standard. Kryptausalgoritmi standardi.
AUTOSAR	AUTomotive Open System Architecture. Ajoneuvoteknisen alan yhteistyöjärjestö.
BMW	Bayerische Motoren Werke AG. Baijerilainen autovalmistaja.
CAM	Cooperative Awereness Message. Viesti, joka sisältää esimerkiksi tilannetietoja liikenteestä.
CRC	Cyclic Redundance Code. Jakolaskuun perustuva tiivistekoodi.
DES	Data Encryption Standard. Kryptausalgoritmi standardi.
ECU	Electronic Control Unit. Elektroninen ohjausyksikkö.
ERP	Enterprise Resource Planning. Toiminnanohjausjärjestelmä.
FAIS	Functional Area Information System. Toiminnallisen alueen tietojärjestelmä.
HSL	Helsingin Seudun Liikenne. Pääkaupunkiseudun julkisen liikenteen operaattori.
IBM	International Business Machine Corporation. Tietokonevalmistaja.
IDS	Intrusion Detection System. Tunkeutumisen havaitsemisjärjestelmä.
IEC	International Electrotechnical Commission. Kansainvälinen sähkötekniikan ja elektroniikan standardointiorganisaatio.
IEEE	Institute of Electrical and Electronics Engineers. Kansainvälinen sähköteknisen alan järjestö.

IEFT	Internet Engineering Task Force. Internet-tekniikkaa kehittävä standardointiorganisaatio.
InfoSec	Information Security. Tietoturvallisuus.
IPS	Intrusion Protection System. Tunkeutumisen estojärjestelmä.
IS	Information System. Tietojärjestelmä.
ISO	International Organization for Standardization. Kansainvälinen standardisointiorganisaatio.
MAC	Media Access Control. Laitteen Ethernet-verkossa yksilöimä koodi.
NHTSA	National Highway Traffic Safety Administration. Yhdysvaltain kansallinen liikenneturvallisuushallinto.
NSA	National Security Agency. Yhdysvaltain kansallinen turvallisuusjärjestö.
OTP	One-Time Pad. Salausalgoritmi.
PUF	Physically Unclonable Function. Fyysisesti kopioimaton menetelmä.
PKI	Public-Key Infrastructure. Julkisten avainten hallintajärjestelmä.
RCF	Request for Comments. IETF:n kehittämiä Internet-standardeja.
RFID	Radio Frequency Identification. Radiotaajuuksilla toimiva etätunnistus.
RSA	Rivest, Shamir, Adleman. Salausalgoritmi.
SHA	Secure Hash Algorithm. Salausalgoritmi.
SAE	Society of Automotive Engineers. Ajoneuvotekninen insinöörijärjestö.
TPM	Trusted Platform Module. Tietoturvalaite tai mikropiiri.

V2I	Vehicle-to-Infrastructure. Tiedonsiirto ajoneuvon ja kiinteän tietoverkon välillä.
V2X	Vehicle-to-X. Tiedonsiirto ajoneuvon ja X:n välillä.
V2V	Vehicle-to-Vehicle. Tiedonsiirto ajoneuvojen välillä.

1 Johdanto

Tämän opinnäytetyön tavoitteena on tutkia ajoneuvojen tietoturvallisuutta kirjallisuuslähteiden kautta, ja luoda aiheesta suomenkielistä materiaalia. Idea opinnäytetyön aiheesta syntyi kuin varkain keskusteltaessa vuodenvaihteessa 2018 esille nousseesta tietokoneiden prosessorien arkkitehtuurillisesta ”virheestä” tietoturvallisuuden näkökulmasta. Keskustelu johti modernien ajoneuvojen sisältämään suureen elektronisten ohjausyksiköiden (prosessorien) lukumäärään jatkuvasti yleistyvissä sähköisissä toimilaitteissa. Näin kiinnostus aiheeseen sekä tarve insinöörityön aiheelle löysivät toisensa.

Ajoneuvojen sähköistyminen on jatkunut kiihtyvänä aina 1900-luvun puolivälistä tähän päivään saakka, eikä kukaan enää katso ällistyneenä kadulla vain rengasmelun säestämänä viilettävää sähköautoa. Aikaisemmin mekaanisina toteutettuja ratkaisuja esimerkiksi ajoneuvojen voimansiirrossa on korvattu sähköisillä komponenteilla, eikä modernissa autossa välttämättä ole mitään fyysistä yhteyttä kuljettajan hallitsemalta ohjausfunktiolta sitä ohjaavalle toimilaitteelle. Sähköistymisen taustalla on visio tulevaisuuden autonomisesta liikenteestä, jossa itsestään ajavat autot korvaavat kuljettajan. Tarkoituksena on parantaa yleistä turvallisuutta ja sujuvuutta liikenteessä, sillä valtaosa liikenneruuhkista ja -onnettomuuksista johtuu inhimillisistä tekijöistä.

Ohjaustoimintojen ja toimilaitteiden sähköistyminen luo kiistämättä monia etuja, mutta kuten kaikella on tälläkin kolikolla kääntöpuolensa. Mekaanisiin toimilaitteisiin vaikuttaminen on käytännössä mahdotonta etäohjatusti, kun taas elektronisesti ohjattujen sähköisten järjestelmien manipulointi ja jopa ajoneuvon etähaltuunotto ja -ohjaaminen ajon aikana on mahdollistunut. Mahdollisuutta ajoneuvojen ohjaus- ja navigointijärjestelmiin vaikuttamiseen suoraan ajon aikana voidaan pitää toimilaitteiden sähköistymisen vakavimpana liikenneturvallisuutta vaarantavana uhkana. Erityisesti uhka kasvaa itseohjautuvien ajoneuvojen tullessa markkinoille ja laajaan käyttöön.

Toinen liikenneturvallisuuteen ja myös ajoneuvojen päästöihin vaikuttava ilmiö on ajoneuvojen ohjausjärjestelmien hakkerointi ja uudelleen ohjelmointi (ns. lastutus). Autojen asetettuja teknisiä suoritusarvoja (moottorin teho, sallittu huippunopeus, pakokaasujen käsittely jne.) voidaan muuttaa elektronisen ohjainlaitteen (ECU) parametrejä muuttamalla. Tällöin ajoneuvot eivät välttämättä enää täytä katsastusvaatimuksia ja vikojen riski kasvaa merkittävästi. Muutoksilla voi olla vaikutusta moottorin ja voimansiirron kestävyyteen ja sitä kautta myös autonvalmistajan takuuvelvoitteisiin. Kolmas merkittävä, lähinnä

valmistajien tekijänoikeuksiin liittyvä ongelma on ajoneuvojen ohjauksessa käytettävien ohjelmistojen helppo kopioitavuus, jolloin autonvalmistaja menettää suurella työpanoksella kehittämänsä ohjelmiston ja samalla kilpailuedun kilpailijalleen.

Lähempänä arkipäivän todellisuutta on ajoneuvojen lokitietojen muuttaminen (esim. matkamittarin lukema, huoltolokit), jolla haetaan suoraan rahallista hyötyä. Tietokoneiden tapaan ajoneuvon lukitseminen ja käytön estäminen ja vapauttaminen lunnaita vastaan on tullut kyberrikollisille mahdolliseksi. Lisäksi sähköisten ajonestojärjestelmien murtamisen haastavuuden kautta ajoneuvovarkauksien luonne on muuttunut ammattimaisemmaksi; uusia ajoneuvoja ei anasteta pelkästään matkanteon helpottamiseksi, vaan autovarkaudet ovat harkittua liiketoimintaa.

Riskien ja vahinkojen minimoimiseksi ajoneuvovalmistajien on muiden tietoteknisten alojen harjoittajien tapaan kiinnitettävä erityistä huomiota tietoturvallisuuteen ajoneuvojen elinkaaren eri vaiheissa. Erityisen tärkeää on hallita tietoturvallisuusriskit ja -uhkat liikenneturvallisuuteen vaikuttavien järjestelmien ja toimintojen osalta. Lisäksi autonomisen liikenteen rakenteiden, kuten tietelematiikan ja muiden älykkään tieverkoston osien, yleistyminen tulevaisuudessa altistaa käyttäjänsä yksityisyyden väärinkäytöksille.

Ajoneuvojen sähköisten ohjausjärjestelmien ja toimilaitteiden yleistymisen myötä ajoneuvotekniikan insinöörille ja erityisesti autosähköinsinöörille on syntynyt tarve ymmärtää sähköisten ohjaus- ja hallintajärjestelmien rakenteita. Järjestelmien suojaamisessa käytettävien tietoteknisten keinojen ja -menetelmien perusteiden ymmärtäminen on huolto- ja tarkastustyötä tekeville insinööreille ja asentajille välttämätöntä.

2 Selvityksen tavoitteet ja toteutus

2.1 Tavoitteet

Tämän selvitystyön tavoitteena on luoda kokonaiskuva tietoturvallisuuskriittisistä ajoneuvoteknisistä sovellutuksista. Aihetta on tarkoitus käsitellä erilaisissa käyttökohteissa ajoneuvon valmistajan, käyttäjän ja mahdollisen hakkerin näkökulmista. Tavoitteena on myös luoda pohjaa suomenkieliselle materiaalille, esimerkiksi autosähkötekniikan koulutuksen tarpeisiin. Selvityksen tarkoituksena ei ole perehtyä erityisen yksityiskohtaisesti aiheen kautta käsiteltäviin teknisiin järjestelmiin, kuten vaikkapa väylätekniikkaan.

Edellä mainittujen tavoitteiden saavuttamiseksi työssä käsitellään muun muassa tietoturvallisuuden sekä kryptologian peruskäsitteitä, toimintaperiaatteita ja ajoneuvojen sisäisten verkkojen tietoturvaratkaisuja ja -ongelmia. Lisäksi tarkastellaan ajoneuvojen keskinäisten sekä tukijärjestelmien verkottumisen luomia hyötyjä ja uhkakuvia sekä ajoneuvojen sähköistymisen ja verkottumisen kautta mahdollistunutta hakkerointia.

Tämä opinnäytetyö nojaa vahvasti aiheesta kirjoitettuun englanninkieliseen materiaaliin. Hankitun tiedon perusteella opinnäytetyössä vastataan seuraaviin tutkimuskysymyksiin:

1. Mihin ajoneuvojen järjestelmien tietoturvallisuus perustuu?

2. Miten ajoneuvojen välinen verkostoituminen vaikuttaa tietoturvan kehitykseen tulevaisuudessa?

3. Millä menetelmillä ajoneuvojen hakkeroinnin riski voidaan minimoida?

Kysymyksen numero 3:n voisi myös muotoilla seuraavanlaisesti: ”Mitä ovat ne keinot, joilla ajoneuvoteollisuus suojaa ajoneuvoja ja asiakastaan tietoverkkojen ja ulkoisten yhteyksien kautta tulevilta hyökkäyksiltä?”

2.2 Selvityksen toteutus

Työssä tiedonhaku pohjautuu pääasiassa aihetta käsitteleviin kirjoihin, verkkohakujen avulla saataviin tiedeartikkeleihin ja täydentäviin alan teollisuuden dokumentteihin. Jälkimmäisten hankkiminen suoraan ajoneuvoteollisuudessa toimivilta yrityksiltä olisi erinomainen tietolähde, mutta loogisesti yritykset suojaavat itseään kilpailulta ja tietovuodoilta pitämällä arkaluonteisen tiedon luottamuksellisena. Yleisiä tietojärjestelmien rakenteita ja niihin liittyvää tietoa ja termistöä on etsitty luotettavista Internet-lähteistä.

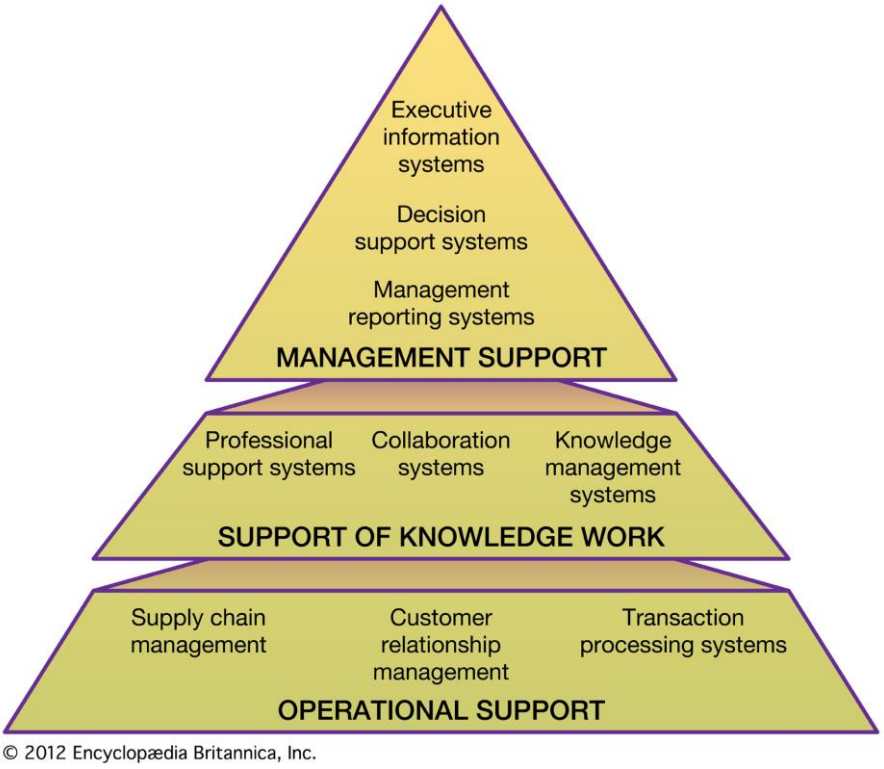
3 Sähköisten järjestelmien tietoturvallisuus

3.1 Tietotekniset järjestelmät ja tietoturvallisuus

3.1.1 Tietojärjestelmän perusmalli

Tietojärjestelmä (Information system, IS) on tiedonkäsittelyn kokoisuus, joka kerää, järjestelee, varastoi ja jakaa tietoa. Tietojärjestelmä -käsitettä käytetään usein virheellisesti puhuttaessa yksittäisestä tietokoneohjelmasta tai -ohjelmistosta, mutta se kattaa tiedonkäsittelylaitteen ja sen sisältämän ohjelmiston lisäksi myös tiedonsiirtoon käytettävät laitteet, käsiteltävän tiedon sekä järjestelmää hyödyntävät ja ylläpitävät tahot, jotka voivat olla muitakin kuin ihmisiä, esim. muita järjestelmiä/laitteita.

Alkujaan tietojärjestelmät jaettiin organisaation hierarkian mukaan pyramidimallisesti tasoihin (kuva 1), jossa alimpana on työntekijöiden hyödyntämät järjestelmät ja ylimpänä johtoportaan käytössä olevat järjestelmät. Aika on kuitenkin ajanut jo tämän mallin ohi, sillä kaikkia nykyisin käytössä olevia tietojärjestelmiä, esimerkiksi datavarastoja tai hakukoneita, ei voi luokitella tämän perinteisen mallin mukaan. [1]



Kuva 1. Tietojärjestelmien pyramidimalli [1].

3.1.2 Tietoteknisen järjestelmän peruskonfiguraatio

Varsinaisista tietokonepohjoisista tietoteknisistä järjestelmistä puhuttaessa tarkoitetaan vastaavaa tietojärjestelmää, jossa hyödynnetään tietojenkäsittelylaitteen laskentatehoa osaan tai kaikkiin järjestelmän suorittamiin tehtäviin. Tietoteknisen järjestelmän peruskomponentit voidaan luokitella seuraavanlaisesti:

- Laitteisto (engl. Hardware)
    - Tiedon näyttämiseen, prosessoimiseen, säilyttämiseen ja hyväksymiseen käytettävät laitteet, esimerkiksi tietokoneen prosessori, muistilaitteet, tulostin, näyttöpääte ja niin edelleen.
- Ohjelmistot (engl. Software)
    - Ohjelmat ja ohjelmistot, jotka mahdollistavat laitteiston käytön, esimerkkinä tietokoneen käyttöjärjestelmä ja sovellukset
- Tietokannat (engl. Databases)
    - Tietojen varastoimiseen ja keräämiseen keskittyvät järjestelmät, esimerkiksi useista kiintolevyistä rakennettu.
- Tietoliikenne (engl. Telecommunications)
    - Tiedon siirtämiseen ja järjestelmän osien yhdistämiseen vaadittavat komponentit, esimerkiksi valokaapeli.
- Henkilöresurssit ja menettelyt (engl. Human resources and procedures)
    - Yllämainittujen komponenttien ohjauskomennot sekä niitä käyttävät ja laativat ammattihenkilöt, esimerkiksi tietotekniikan insinööri.

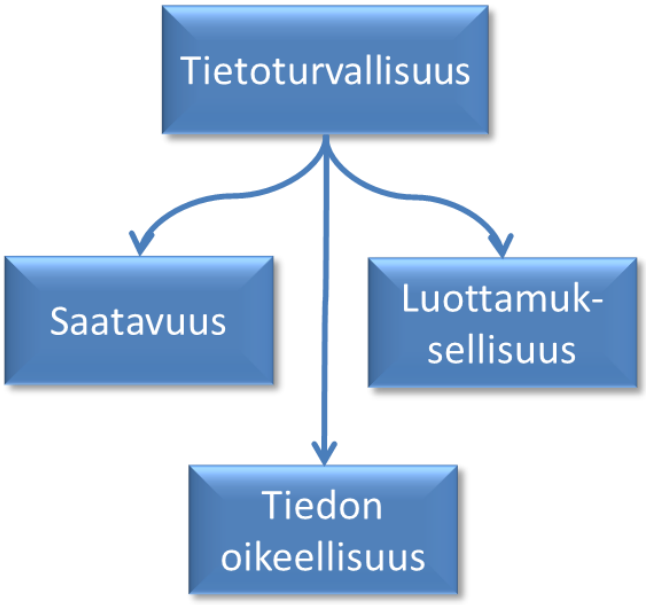
Laitteistot, ohjelmistot, tietokannat ja (lähi)verkot muodostavat niin kutsutun tietoteknisen alustan, jota hyödyntämällä voidaan luoda halutunlainen tietojärjestelmä. Useiden tietojärjestelmien, päätelaitteiden ja tietoliikenneverkkojen muodostamasta kokonaisuudesta

käytetään usein nimitystä tietoverkko, esimerkiksi Internet. Lienee selvää, että tietoteknisiä järjestelmiä toimii hyvin monilla eri tasoilla, aina organisaation tietyn osan spesifisestä järjestelmästä organisaatioita yhdistäviin järjestelmiin asti. Organisaatioiden tiettyjen osien tukijärjestelmiä kutsutaan toiminnanohjausjärjestelmiksi (enlg. ERP, Enterprise Resource Planning). Näihin järjestelmiin lukeutuvat muiden muassa esimerkiksi tilikirjanpito-, tuotannonohjaus-, markkinointi-, ja henkilöstöosastojen tarpeisiin luodut tietojärjestelmät. [1]

3.1.3 Tietoturvallisuuden termistöä ja yleinen määritelmä

Tietoturvallisuus (engl. Information Security, InfoSec) on termi, jota käytetään kuvaamaan tilaa, jossa kaikki arvokkaat tiedot suojataan luvattomalta käytöltä. Tarkoituksena on suojata asianomaista järjestelmää ja sen käyttäjää/käyttäjiä, kuten esimerkiksi tässä tapauksessa autoa ja sen kuljettajaa sekä mahdollisia matkustajia, erilaisilta tietojärjestelmään kohdistuvilta virheiltä, hyökkäyksiltä ja manipulaatioyrityksiltä. Tietoturvalla mahdollistetaan jonkin taho, yrityksen tai organisaation, toiminta estämällä tietojärjestelmän kaikenlainen luvaton hyväksikäyttö; tiedon luvattomasta lukemisesta tiedon muuttamiseen ja tallentamiseen sekä tuhoamiseen. [3]

Yleisesti tietoturvallisuudella tarkoitetaan kolmea tiedon ominaisuutta ja niiden ylläpitoa. Nämä tekijät ovat kuvassa 2 nähtävät tiedon saatavuus, tiedon luottamuksellisuus ja tiedon oikeellisuus eli eheys.

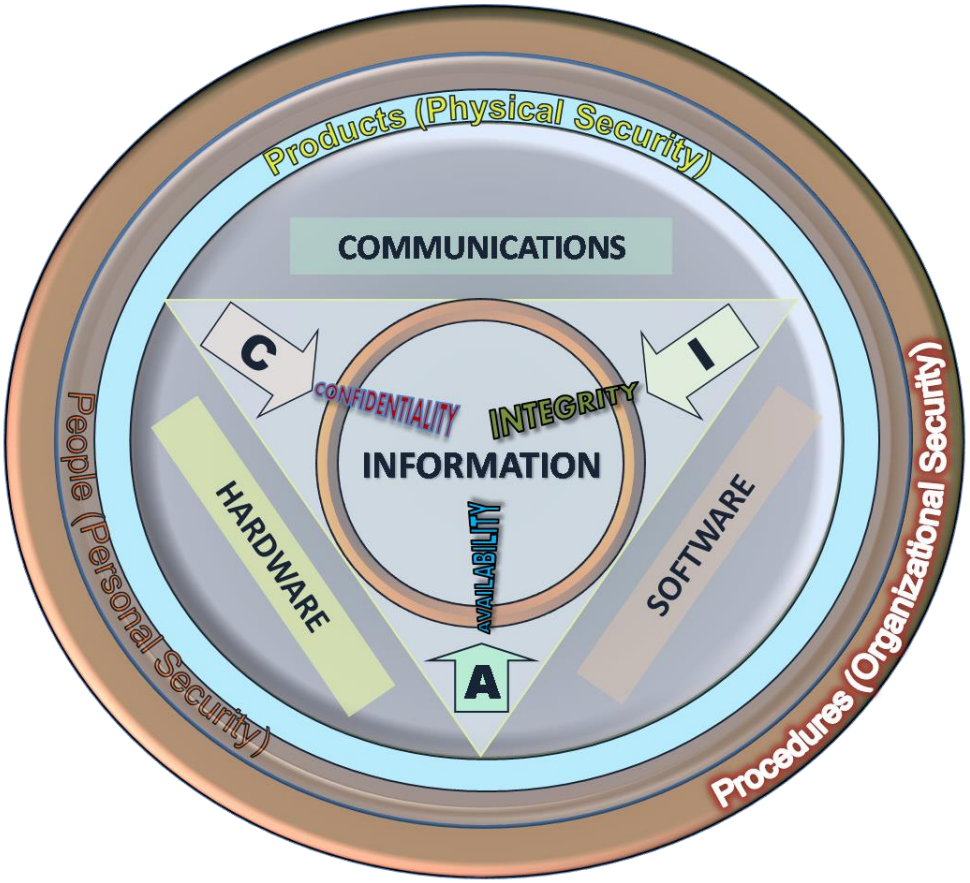


Kuva 2. Yleisiä tietoturvallisuuden käsitteitä.

Suomenkielessä käytetään yleensä englanninkielisistä turvallisuustermeistä Safety ja Security vain yhtä sanaa ”turvallisuus”. Safety-termi liittyy lähinnä saatavuuteen (toimintavarmuus) ja ulkoiseen turvallisuuteen ja on siten voimakkaasti sidoksissa teknisiin ratkaisuihin ja toimintojen varmennuksiin, esimerkiksi turvavyö = safety belt. Security termi kuvaa fyysistä ja aineetonta suojaamista, esimerkiksi tietoturvallisuus = information security.

- Saatavuus tai käytettävyys (engl. Availability)
    - Tieto, järjestelmä tai palvelu on oikeutettujen käyttäjien käytettävissä haluttuna hetkenä [2].
- Luottamuksellisuus (engl. Confidentiality)
    - Tieto tai järjestelmä on vain ja ainoastaan oikeutettujen tahojen käytössä [2].
- Eheys (engl. Integrity)
    - Tietoa ei ole luvattomasti muutettu eikä se ole päässyt virheellisesti muuttumaan, eli korruptoitumaan [2].

Näiden tietoturvallisuusomaisuuksien (engl. Information Security Attributes) englanninkielisten termien pohjilta on luotu ytimekäs kirjainyhdistelmä ja edellä mainitut ominaisuudet tunnetaankin kuvassa 3. nähtävänä CIA-kolmikkona (CIA Triad of Information Security). Perinteisesti tietoturva on määritelty turvallisuuspäämäärien kautta ja kyseinen kolmikko on 1970-luvulta asti liittynyt oleellisesti tietoturvallisuuteen [5, s. 11]. Tässä esityksessä on rajauduttu tarkastelemaan tietojärjestelmän kolmea keskeistä osaa: laitteistoa, ohjelmistoa ja yhteyksiä.



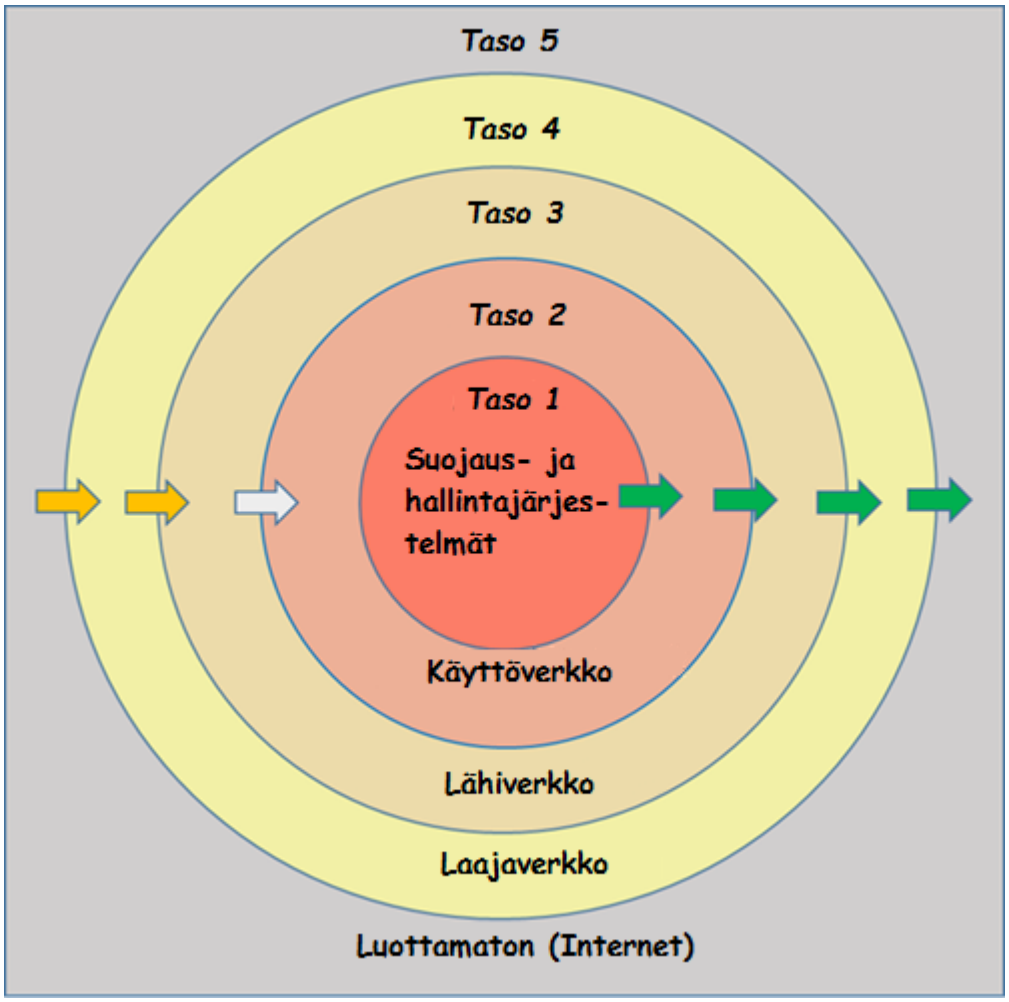
Kuva 3. CIA Triad of Information Security [4].

Kolmikon sisäinen suhde riippuu hyvinkin paljon käyttötarkoituksesta, perinteisesti auton tapauksessa päällimmäiseksi voisi nostaa tiedon saatavuuden (auto on käytettävissä,

sillä hetkellä, kun sitä tarvitaan). Tosin puhuttaessa modernista ajoneuvosta korostuvat myös luottamuksellisuuden ja eheyden roolit (vrt. liikenneturvallisuus).

3.1.4 Tietojärjestelmän suojaaminen

Tietojärjestelmien suojaamisessa on yleisesti käytössä kuvassa 4 nähtävä vyöhykesuojausmalli (engl. Defence-in-Depth), jossa suojattava kohde on useiden, eri tavalla rakennettujen suojavyöhykkeiden sisällä. Malli pätee erityisesti toimistoympäristöjen tietojärjestelmien suojaamiseen ja on hyvin sovellettavissa myös automaatioympäristöjen tietojärjestelmien (prosessinohjausjärjestelmien) suojaamiseen ulkoisilta tietoturvauhkilta.



Kuva 4. Tietoturvallisuuden vyöhykesuojausmallin (Defence-in-Depth) -periaate.

Seuraavassa on listattu joitain tyypillisiä käytännön tietoturvavälineitä ja työkaluja tietoturvan varmistamiseksi:

Tietojärjestelmien ja niiden käyttäjien suojaamiseksi luottamuksellinen tieto on pidettävä salassa. Tiedon päätymistä vääriin käsiin ennalta ehkäistään suojaamalla tietojärjestelmä luvattomalta käytöltä ja ulkoisilta hyökkäyksiltä käyttämällä erityisiä suojausjärjestelmiä ja menetelmiä:

- Palomuurit (engl. Firewall)
    - Suojaa tietojärjestelmää valvomalla tietoliikennettä ja pyrkimällä estämään pääsy ja tiedon luvaton kulku tietoverkkojen, esimerkiksi Internetin ja organisaation sisäisen verkon, välillä käyttäen ennalta määriteltyjä sääntöjä. [6]

- Tunkeutumisen havaitsemis- ja estojärjestelmät (engl. Intrusion Detection System, IDS ja Intrusion Protection System, IPS)
    - Valvoo tietojärjestelmässä tai -verkossa liikkuvaa dataa. Havaitsevat epänormaaleja tapahtumia ja kirjaavat tarvittavat tiedot raporttien tuottamiseen ja lähteen sekä mahdollisen tunkeutumisen luonteen määrittämiseen. Aktiivisemmilla järjestelmillä (IPS) pyritään myös estämään tunkeutuminen havaitsemisen jälkeen reaaliajassa. [1, s. 6]

- Sovellutusten salliminen (engl. Application whitelisting)
    - Erityinen tietoturvasovellus valvoo, että ainoastaan ennalta määriteltyjä sovelluksia ajetaan tarkasteluympäristössä, esimerkiksi palvelin tai mikrokontrolleri.

- Haavoittuvuusskannerit (engl. Vulnerability Scanners)
    - Arvioi tietokoneen, -järjestelmän tai -verkon ja käyttöjärjestelmän sekä ohjelmistosovellusten erilaisia heikkouksia [7]. Esimerkkinä virustorjuntaohjelmistot.

- Tietojärjestelmän koventaminen (engl. System Hardening)
    - Tietojärjestelmästä poistetaan kaikki perustehtävään kuulumattomat ja tarpeettomat sovellukset, tietoliikenne- ja USB-portit yms.
- Tietojen salaaminen (engl. Data Encryption)
    - Tietojärjestelmän kriittinen ja luottamuksellinen tieto salataan, katso tarkemmin kohta 3.2.
- Tunnistus- ja autentikointijärjestelmät
    - Käyttäjien tunnistus- ja autentikointijärjestelmillä valvotaan sekä sisäisten että ulkoisten käyttäjien pääsyä tietojärjestelmään ja hallitaan muun muassa käyttäjälistoja, salasanoja ja muita tunnistamis- ja käyttöoikeustietoja.
    - Voidaan käyttää viestin tai ohjelmiston oikeellisuuden todentamiseen (digitaaliset sertifikaatit, allekirjoitukset).

Edellä mainituilla tietoturvamenetelmillä ja -työkaluilla pyritään estämään luvaton pääsy järjestelmään ja sen sisältämiin tietoihin. Kuitenkaan nämä eivät aina takaa absoluuttista suojaa tunkeilijoita vastaan. Tämän vuoksi tietojärjestelmien toimintakriittinen ja luottamuksellinen tieto voidaan salata salauskoodin avulla eli kryptata. Tyypillisesti tietojärjestelmissä salattua tietoa ovat erilaiset salasanat, varmenteet, järjestelmälokit, langaton tiedonsiirto ja toimintakriittiset tietokannat, esimerkiksi järjestelmän parametrointitietokanta.

3.2 Kryptologia eli tietojen salaaminen

Kryptologia on tieteen ala, joka tutkii salakirjoitustekniikoita. Kryptologian juuret löytyvät syvältä sivistyksen ja yhteiskuntajärjestyksen alkuajoilta, ja itse termi onkin peräisin kreikan kielisistä sanoista *kryptós* (“kätketty”) ja *lógos* (“sana”). Käsitteenä kryptologia sisältää kaksi osaa, kryptografia ja kryptoanalyysi.

Kryptografia tarkoittaa tiedon salaamiseen perehtynyttä tieteenalaa, jonka tarkoituksena on tutkia ja kehittää tapoja piilottaa tietoja luvatonta käyttöä vastaan. Vastaavasti kryptoanalyysi tutkii tapoja murtaa salakirjoitus ja hankkia tietoja järjestelmistä luvatta. [8]

Kryptografia ja kryptoanalyysi ovat eräänlaisessa symbioosissa: kryptoanalyysi on välttämätön ala kryptograafisten menetelmien turvallisuuden varmistamiseen sekä uusien menetelmien tutkimiseen ja kehittämiseen [9, s. 13]. Selkokielellä se tarkoittaa käytettyjen salausten murtamista ja vahvempien salausten kehittämistä tämän pohjalta.

Kryptografian muodostavat tiedon salaamiseen (engl. Encryption) ja salauksen purkamiseen (engl. Decryption) käytettävät toimintaproseduurit, algoritmit. Nämä algoritmit puolestaan jakautuvat kahteen osioon, symmetrisiin (engl. Symmetric-key algorithms) sekä epäsymmetrisiin (julkisiin) algoritmeihin (engl. Asymmetric-key algorithms). [9, s. 13.]

3.2.1 Symmetrisen avaimen kryptografia

Wolf tiivistää symmetristen avainten kryptografiaa väitöskirjassaan seurvaavanlaisesti: ”Symmetrisen avaimen kryptograafiset algoritmit ovat perusrakennuspalikoita jokaisessa turvallisessa järjestelmässä, joka vaatii vähintään luottamuksellisuutta. Niitä käytetään viestien massakryptaamiseen ja ne tarjoavat turvallisen tavan varastoida dataa.” Tekstissään ajoneuvojen tietoturvallisuudesta väitellyt Wolf myös vertaa kyseistä menetelmää lukittuun laatikkoon, jonka sisällä viestit ovat. Laatikko lähetetään ja oikealla avaimella se saadaan avattua ja sisältö luettua. Symmetrisen avaimen turvallisuus on riippuvainen sen kryptograafisesta vahvuudesta, jonka puolestaan määrittää avaimen pituus ja käytetty algoritmistandardi. [9, s. 14.]

Käytetyimpiä julkisia algoritmistandardeja ovat DES (Data Encryption Standard) ja AES (Advanced Encryption Standard):

- Data Encryption Standard (DES)
    - International Business Machines Corporationin (IBM) luoman “Lucifer”-algoritmin pohjalta Yhdysvaltain Kansallisen turvallisuusviraston (National Security Agency, NSA) salassa kehitetty lohkopituudeltaan 64-bittinen (avain 56-bittinen) salausalgoritmi. Julkaistu vuonna 1977. [10]

- Advanced Encryption Standard (AES)

    - Yhdysvaltain kansallinen standardi- ja teknologiainstituutti (engl. National Institute of Standards and Technology, NIST) lähetti vuonna 1997 julkisen pyynnön kehittää uusi standardi korvaamaan ikääntynyt DES. Vuonna 2000 uudeksi standardiksi valikoitui kahden belgialaisen kryptograafikon luoma Rijndael -algoritmi. [11] AES mahdollistaa 128-, 192-, ja 256-bittisten avainten käytön. Lohkopituus standardissa on 128 bittiä. [12]

Aika on auttamattomasti ajanut DES-standardin ohi, sillä tänä päivänä koodi murtuu alle yhdeksässä minuutissa, kun suoritetaan perusteellinen avainhaku siihen tarkoitetulla erikoislaitteella. Hintaa tällaisella laiteella on alle 10 000 €. Tosin DES:stä on kehitetty eri variaatioita ja kolminkertaista DES:n mukaista kryptausta (Triple-DES) voidaan turvallisesti käyttää tänäkin päivänä. AES:n mahdollistamien eripituisten salausavainten ansiosta voidaan valita haluttu avainpituus ja sitä kautta saavuttaa eri kohteille niihin sopiva tietoturvallisuuden taso. [9, s. 14–16.]

AES ja DES ovat molemmat lohkoihin perustuvia salauksia (engl. Block cipher). Käytännössä tämä tarkoittaa sitä, että data kryptataan 64- tai 128-bittisissä osissa. Käytössä on myös jokaisen yksittäisen bitin kryptaamiseen perustuvia symmetrisen avaimen algoritmeja (engl. Stream cipher). Tunnetuin näistä on One-Time Pad (OTP) -salaus, joka myös Vernam -salauksena tunnetaan. OTP on ainoa yleisesti tiedossa oleva murtamattomaksi todistettavissa oleva salausmenetelmä. Se on kuitenkin ongelmallinen, koska salauksen avaaminen vaatii lähetetyn viestin pituisen salausavaimen lähettämistä. Joka tapauksessa vastaavia salauksia hyödynnetään sellaisissa sovelluksissa, joissa virheet tiedonsiirrossa ovat todennäköisiä, sillä jokaisen bitin erikseen kryptaaminen estää virheiden leviämisen datavirrassa, eli virhe ei pääse korruptoimaan kuin yhden bitin. Myös matalan laitemuistin ja/tai laskentatehon sovelluksissa voidaan käyttää OTP- tai vastaavaa salausta menestyksekkäästi. [9, s. 15.]

3.2.2 Epäsymmetriset algoritmit eli julkisen avaimen kryptografia

Modernien tietoverkkojen, erityisesti Internetin, toiminta perustuu epäsymmetrisiin (julkisen avaimen, PKI, Public Key Infrastructure) salausalgoritmeihiin pohjautuviin protokolliin. Esimerkkejä jo perinteisistä epäsymmetrisistä salausalgoritmeistä ovat Diffie-Hellman-avaimenvaihtoprotokolla sekä RSA- ja ElGamal-salausalgoritmi.
Epäsymmetriset salausalgoritmit perustuvat usein kahteen avaimeen, joista toinen on julkinen ja toinen yksityinen (salainen). Avaimet ovat esimerkiksi RSA-järjestelmässä ovat kahden erittäin suuren alkuluvun tulon tekijöitä. Alkulukujen kertominen on helppoa, mutta tulon jakaminen tekijöihin käytännössä mahdotonta. Haluttu viesti salataan julkisella avaimella ja puretaan käyttäen julkista ja yksityistä avainta.

RSA-agroritmia voidaan käyttää myös viestin allekirjoittamiseen. Alkuperäisestä viestistä lasketaan ensin tiivistefunktio käyttäen tiivistealgoritmia (HASH-algoritmi, esimerkiksi SHA-1) ja saatu tiiviste salataan käyttäen SHA-salausavainta. [9, s.19-20]

Usein käytetään menettelyä, jossa salausavain lähetetään käyttäen epäsymmetristä salausta ja varsinainen suojattavan tiedon salaus tehdään tehokkaalla symmetrisellä salauksella, esimerkiksi AES256.

3.2.3 Tiivistefunktiot (HASH-funktiot)

Tiedonsiirrossa on jo pitkään käytetty erilaisia varmenteita siirretyn datayksikön (tyypillisesti tavu tai kehys) muuttumattomuuden tarkistamiseen. Esimerkiksi pariteettitarkistusmenetelmä on alkeellinen ja haavoittuva, mutta varsin tehokas pienten tietoyksiköiden (tavu) virheentarkistusmenetelmä.

Varsinaisia tehokkaita tiivistefunktioita käytetään kooltaan suuremman viestin tai tietoblokin (tietopaketti) allekirjoitukseen. Allekirjoituksella voidaan varmentaa viestin aitous eli muuttumattomuus. Erilaisia tiivistefunktioiden laskenta-algoritmeja on useita, joista voisi mainita esimerkiksi CRC- (Cyclic Redundancy Check) ja SHA-1-menetelmät. Tällaisia tiivistefunktioita käytetään esimerkiksi autojen elektronisten ohjausyksiköiden (ECU, Electronic Control Unit) parametrikarttojen ja ohjelmien tiivisteiden laskemiseen sekä elektronisten lukitusjärjestelmien avainten todentamiseen. [9, s. 27–28.]

3.3 Tietoturvallisuusstandardit ja normit

3.3.1 Yleiset tietoturvastandardit ja standardointitahot

Tietoturvallisuuden ja sähkötekniikan kannalta tärkeitä kansainvälisiä standardointielimiä ovat ISO (International Organization for Standardization) ja IEC (International Electrotechnical Commission). Järjestöt tuottavat ja julkaisevat yhdessä erittäin laajasti standardeja lähes kaikilta tekniikan alueilta mukaan luettuna sähkötekniikka ja tietoturvallisuus. Liitteessä 1 on esimerkkinä lueteltu ISO/IEC 27000 -sarjan tietoturvallisuusstandardeja. Varsinainen autojen kyberturvallisuuden ISO-standardi (ISO/SAE AWI 21434) on vasta kehitteillä. [16]. Standardit ovat maksullisia, ja Suomessa niitä välittää SESKO ry (Suomen sähköteknillinen standardisointiyhdistys).

Kaksi muuta merkittävää tietojärjestelmien ja tietoturvallisuuden standardointitahoa ovat yhdysvaltalainen IEEE (Institute of Electrical and Electronics Engineers) sekä Internet-standardointia tekevä IETF (Internet Engineering Task Force). Ensin mainittu julkaisee mm. IEEE-standardeja ja jälkimmäinen RFC-suosituksia. [29]

3.3.2 Ajoneuvoteknisen alan tietoturvallisuusstandardit ja -normit

Kuten edellä mainittiin, ei ajoneuvotekniselle alalle ole vielä julkaistu kansainvälisiä tietoturvallisuusstandardeja. Kyseisen ISO/SAE AWI 21434 -standardin status ”Under development” (suom. kehitteillä) implikoi kuitenkin, että ajoneuvojen tietoturvallisuuden puutteeseen on herätty ja asialle tehdään jotakin. Nähtäväksi jää standardin vaikutus ajoneuvoteollisuudessa yleisesti ja vaikkapa autojen linkittymiseen Internetin ynnä muiden tietoverkkojen kanssa. Kansainvälinen ajoneuvotekniikan insinöörien järjestö SAE International (Society of Automotive Engineers) on julkaissut vuonna 2016 Kyberturvallisuutta käsittelevän ohjekirjan, joka kantaa nimeä ”Cybersecurity Guidebook for Cyber-Physical Vehicle Systems”. Se on merkitty standardiksi tunnuksella ”J3061_201601”. Teos antaa lähinnä sellaista tietoa, jolla voidaan jalostaa alalla toimivan yrityksen proseduureja ja toimintamalleja tietoturvallisempaan suuntaan prosessikehyksen koko elinkaaren aikana. [19] Lisäksi SAE on määritellyt standardilla J2945/1 ajoneuvojen välisen yhteysprotokollan.

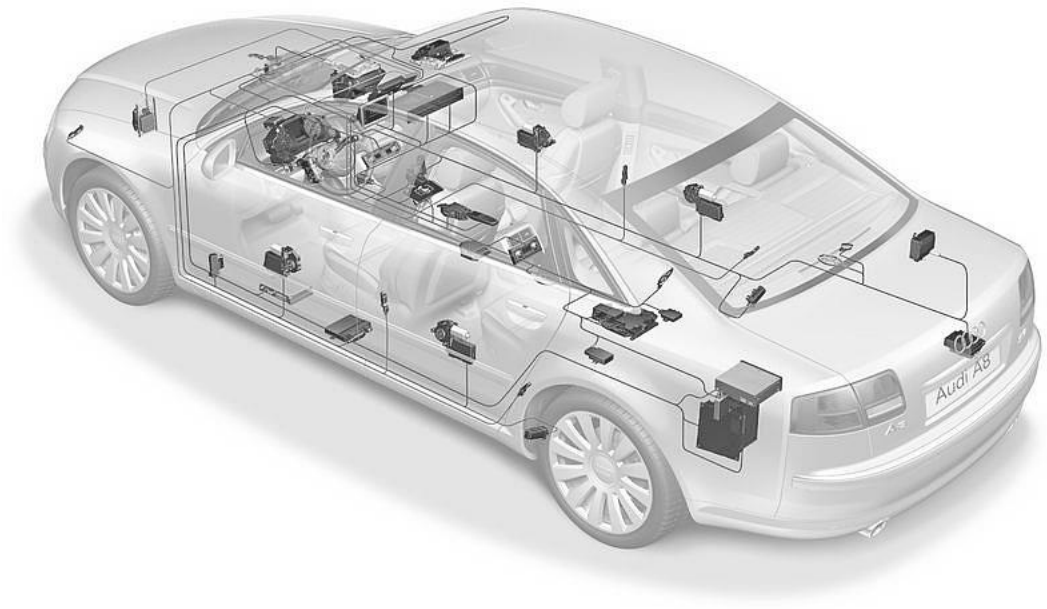
Kansainvälisiä autoalan tietotekniikan normeja ja spesifikaatioita laatii mm. auton- ja osavalmistajien yhteinen järjestö AUTOSAR (Automotive Open System Architechture).

Järjestön tavoitteena on luoda standardisoitu rajapinta ajoneuvoteollisuudessa käytettävien sovellusten ja elektronisten ohjausyksikön (ECU) välille. Tämän kautta AUTOSAR pyrkii takaamaan ajoneuvovalmistajien tietoturvallisuuden esimerkiksi ylläpitämällä ohjelmistopäivitysten saatavuutta. Muita järjestön kotisivuilla mainittuja tavoitteita ovat lisätä osavalmistajien komponenttien sekä ohjelmistojen penetraatiota tuotelinjojen yli, parantaa ohjelmistojen uudelleenkäytettävyyttä, nopeuttaa kehitystä sekä ylläpitoa, hallita tuotteiden sekä prosessien kehitystä monimutkaisuuden ja riskien minimoimiseksi ja skaalattavien järjestelmien kustannusten optimointi. AUTOSARin ydinpartnereita ovat BMW Group, Robert Bosch GmbH, Continental AG, Daimler AG, Ford Motor Company, General Motors, PSA Group, Toyota ja Volkswagen AG. Lisäksi järjestöön kuuluu lukuisia muita ajoneuvo-, komponentti- ja ohjelmistovalmistajia kehitys- ja yhteistyöpartnereina. [17]

4 Tietoturvallisuus ja ajoneuvot

4.1 Ajoneuvojen tietotekninen rakenne

Nykyaikainen poltto- tai sähkömoottorikäyttöinen ajoneuvo on lukuisten elektronisten ohjausyksiköiden (ECU), toimilaitteiden ja sensorien muodostama tietojärjestelmä, jossa ohjausyksiköt on liitetty toisiinsa tietoliikenneväylällä. Ohjausyksiköt ohjaavat ja lukevat yleensä niihin suoraan kytkettyjä toimilaitteita ja sensoreita. Nykyisissä moderneissa hyvin varustelluissa autoissa saattaa olla toista sataa ohjausyksikköä. Yleensä ohjausyksikön sydämessä toimii RISC-prosessori (RISC, Reduced Instruction Set Computer), esimerkiksi ARM- tai Cortex-suoritinperheen jäsen. [9, s. 72.] Oheisessa kuvassa 5 on visualisoitu henkilöauton tietojärjestelmää.



Kuva 5. Audi A8 -henkilöauton ohjausyksiköitä ja väyliä [9, s. 72].

Ajoneuvojen ohjausyksiköissä on harvoin erillistä käyttöjärjestelmää. Ohjausyksikköön ladattava ohjelmisto sisältää kaikki ohjausyksikön toiminnassa tarvittavat toiminnallisuudet. [13, s. 31–32.] Tietoturvan kannalta asiassa on sekä hyviä että huonoja puolia.

Hyvistä puolista mainittakoon, että näihin ohjelmistoihin eivät pysty vaikuttamaan tavanomaiset, toimisto- ja henkilökohtaisille tietokoneille vaaralliset haittaohjelmat tai murtotyökalut. Toisaalta karsitussa ohjausyksikön ohjelmistossa ei ole mitään edistyksellisiä ominaisuuksia, joilla havaittaisiin tai voitaisiin estää ohjausyksikköön kohdistuva hyökkäys (ks. 3.1.4). [29]

Ajoneuvoväylät ovat tyypillisesti yksinkertaisia yhdestä tai kahdesta metalliparikaapelista muodostettuja, sarjamuotoista liikennöintiä käyttäviä yhdyskäytäviä. Ajoneuvoväylissä käytetään erilaisia tietoliikenneprotokollia riippuen ajoneuvon valmistajasta, iästä ja mallista. Esimerkkeinä nykyisin käytössä olevista väylästandardeista mainittakoon CAN-väylä (Controller Area Network, ISO 11898), LIN-väylä (Local Interconnect Network, ISO 17987) sekä FlexRay (ISO 17458). Tyypillistä ajoneuvoväylille on reaaliaikainen, suhteellisen hidas tiedonsiirto (20 kbit/s – 10 Mbit/s) sekä yhteiskäyttöperiaate. Yhteiskäyttöperiaatteella tarkoitetaan sitä, että samaan väylään on kytketty useita ohjausyksiköitä, joista jokainen voi liikennöidä omasta aloitteestaan ilman muiden laitteiden ohjausta. Liikennöinti tapahtuu siis ilman keskitettyä kontrollia. Edellä mainituista väylistä CAN- ja LIN-väylät käyttävät asynkronista tiedonsiirtoa, kun sitä vastoin FlexRay-tiedonsiirto on synkronista (prosessorin kellosignaaliin tahdistettua). Erillisiä tietoliikenneväyliä on ajoneuvoissa yleensä useita eri käyttötarkoitukseen, tyypillisesti 3–5 kpl. Esimerkiksi moottorin, vaihteiston ja jarrujen ohjausyksiköt voivat olla samassa väylässä. Lisäksi tiedonsiirtonopeus eri väylillä voi vaihdella.

Ajoneuvon tietojärjestelmään liitytään huoltoa varten OBD-väylän (OBD, On-Board Diagnostics) kautta. Alkujaan se oli erityisesti pakokaasupäästöjä kasvattavien vikojen havainnointiin, tallentamiseen sekä vioista ilmoittamiseen käytetty järjestelmä. OBD tarkkailee sensorien tuottamien signaalien arvoja sekä eheyttä. Vikatilanteet tallennetaan ja niistä voidaan ilmoittaa kuljettajalle sytyttämällä vikavalo kojetaulussa. Pahimmissa tapauksissa OBD voi estää joitakin auton funktioita, esim. ”limp-home”-tila rajoittaa mottorin kuormittamista. OBD:n tehtävä on siis pääasiassa tunnistaa vikatilanteita ajoneuvon sähköjärjestelmässä. OBD:n on oltava jonkin väylän kautta yhteydessä johonkin ohjainlaitteeseen, tyypillisesti CAN-väylää tai K-linjaa hyödyntäen. OBD-pistokkeen on mahdollista lähettää CAN-viestejä, mutta yleisesti vain diagnostiikkaa pyörittävälle ohjainlaitteelle.

Nykyaikaisissa ajoneuvoissa on OBD-väylän lisäksi muitakin ulkoisia yhteyksiä, jotka mahdollistavat ainakin teoriassa hyökkäyksen ajoneuvon tietoverkkoon. Tällaisia yhteyksiä ovat esimerkiksi valmistajien pilvipalveluihin rakennetut yhteydet ja onnettomuustilanteissa aktivoituvat hätälähetinyhteydet. Viimeksi mainitut on toteutettu julkisten matkaviestinverkkojen avulla. Kaikki ulkoiset yhteydet ajoneuvosta ulkoisiin järjestelmiin luovat potentiaalisen uhkan ajoneuvon tietoturvalle ja tietojen yksityisyydelle. Huomautuksena Euroopan unionin 25.5.2018 voimaan tuleva tietosuojauudistus, joka asettaa rekisterinpitäjälle velvollisuuksia käyttäjätietojen hallintaan. [21]

4.2 Ajoneuvojen tietoturvateknisen rakenteen kehittyminen

Tietoturvallisuus ajoneuvoissa on tärkeää jo nyt, mutta erityisesti tulevaisuudessa. Ajoneuvojen tietoturvaratkaisuja pyritään kehittämään standardiratkaisujen pohjalta (kohta 3.2.2), mutta standardointityö on edennyt liian hitaasti muun autokehityksen tarpeisiin nähden. Ajoneuvot ovat kovaa vauhtia kehittymässä automaatiojärjestelmien viime vuosikymmeninä näyttämään suuntaan. Ajoneuvoalalla tämä tarkoittaa käytännössä muun muassa pitkälle kehittyneitä ajonhallintajärjestelmiä ja itseohjautuvia autoja. Tämän vuoksi ajoneuvovalmistajat korvaavat komponentti kerrallaan ajoneuvojen hallintalaitteistojen mekaanisia ratkaisuja sähköisillä vastineilla. Epäyhtenäinen toteutus on johtanut puutteelliseen tietoturvallisuuden kokonaishallintaan, joita tämän dokumentin johdannossakin esimerkein mainittiin. Laadukas tietoturva ei kuitenkaan vain takaa matkustajille sekä muille tienkäyttäjille turvallista matkantekoa, vaan se myös avaa alalle täysin uusia liiketoimintamahdollisuuksia.

Rahan ansaitsemisen ja asiakkaiden elossa pitämisen lisäksi tietoturvallisuuteen liittyy kolmaskin näkökulma, ajoneuvojen luotettavuus. Sähköiset järjestelmät pystyvät tarkastelemaan omaa ja muiden sulautettujen järjestelmien toimintaa, ilmoittamaan vikatilanteista ja jopa diagnosoimaan vian syitä. Tietenkään sähköistyminen ei takaa absoluuttista faktatietoa järjestelmän tilasta, vaan sen selvittäminen voi vaatia hyvin perehtyneen mekaanikon, esimerkiksi autosähkötekniikan insinöörin, ammattitaitoa. Toisaalta hyvin yksityiskohtaisten järjestelmätietojen jakaminen ja levittäminen myös mahdollistaa epärehellisten ja laittomien liiketoimintamallien omaksumisen jopa alan ammattilaisten keskuudessa.

4.3 Ajoneuvojen liittäminen tietojärjestelmiin

Yhteydet erilaisiin pilvipalveluihin lisääntyvät tulevaisuudessa voimakkaasti ajoneuvoalalla. Tällaisia pilvessä olevia palveluja ovat muun muassa autonvalmistajien palvelut, tulevaisuuden liikenteenohjauspalvelut, kuljetustenohjauspalvelut, tiesääpalvelut, sähköautojen latauspalvelut, yhteydet sertifiointipalvelimille jne. Palveluilla voidaan muun muassa ennakoida ja havaita ajoneuvon huoltotarvetta, vähentää liikenneruuhkia, optimoida kuljetuksia sekä vähentää ympäristöpäästöjä.

Tietoverkkoon yhteydessä olevien ajoneuvojen ja älykkään tieverkoston infrastruktuurin välinen tiedonsiirto mahdollistaa liikenteenohjauksen reaaliajassa. Tämän kaltainen ”Vehicle-to-X” (V2X) -kommunikaatio voi myös tapahtua ajoneuvojen välillä (”Vehicle-to-Vehicle”, V2V) tai ajoneuvon ja infrastruktuurin (esim. tietelematiikan) välillä. Viimeisintä kutsutaan samalla tyylillä ”Vehicle-to-Infrastructure”- eli V2I-kommunikaatioksi. V2X-kommunikaation odotetaan parantavan liikenteen turvallisuutta ja yleistä sujuvuutta ja mukavuutta tulevaisuudessa huomattavasti. Ajoneuvot lähettävät ja vastaanottavat toisiltaan CAM (Cooperative Awareness Message) -viestejä, jolloin ne saavat tietoa toistensa liikkeistä. Tämän avulla voidaan esimerkiksi varoittaa törmäyskurssilla olevista ajoneuvoista ja jopa käyttää autonomista jarruttamista onnettomuuden estämiseen. [14, s. 1.]

Modernissa autossa voi olla, sen sisältämien useiden eri sensoriteknologioiden ansiosta, kehittynyt ympäristön havainnointijärjestelmä. Tällaisten järjestelmien päälle rakennetut aktiiviset turvajärjestelmät, kuten adaptiivinen vakionopeudensäädin tai autonominen jarrutus, ovat jo tehneet autoilusta turvallisempaa. Jo valmiiksi autosta löytyvää tekniikkaa voisi ajoneuvojen verkottumisen kautta hyödyntää enemmän. Kun ajoneuvojen havainnointijärjestelmään integroidaan ruuhkatietoja tai muita poikkeusolosuhteita rekisteröiviä ohjelmistoja ja välitetään niiden luomaa informaatiota muille tienkäyttäjille reaaliajassa, voidaan saavuttaa hyvinkin positiivinen vaikutus sekä liiketeen yleiseen turvallisuuteen, että sujuvuuteen.

Toisaalta älykkään tieverkoston luomiseen vaadittavan liikennetelematiikan tuottaman valtavan datamäärän hallitsemiseen varmasti tarvitaan tehokas ja pääosin reaaliaikainen tietojärjestelmä. Järjestelmän on oltava tietoturvallinen, ja sen pitää pystyä estämään verkon kaikenlainen väärinkäyttö. Tämä vaatiikin kryptologisten menetelmien käyttöä viestien oikeellisuuden varmistamiseksi ja manipuloinnin estämiseksi. [14, s. 2.]

”Turvallisuuden ohella myös yksityisyyteen on kiinnitettävä huomiota: paikkatiedot ovat hyvin arkaluontoisia, sillä meidän liikkumisemme paljastaa meistä paljon (esimerkiksi kodin ja työpaikan sijainnit) käyntikohteidemme tunteminen mahdollistavat päättelyn meidän henkilökohtaisista ja poliittisista mielipiteistä”, toteaa Förster väitöskirjassaan. Tämä ei pelkästään koske järjestelmän ulkopuolisten tahojen harjoittamaa tietojen kalastelua V2X-viestinnän perusteella, vaan myös järjestelmää ylläpitävät tahot pääsevät käsiksi dataan, joka uhkaa käyttäjän yksityisyyttä. Järjestelmän operaattorilta turvautuminen voi tuntua hullulta, mutta valtavan yksityisyyttä uhkaavan datamäärän säilöminen, esimerkiksi pilvipalveluihin, houkuttelee motivoituneita hyökkääjiä. Ongelmaa kuitenkin mutkistaa entisestään V2X-viestinnän luonne: dataa lähetetään hyvin tiheällä frekvenssillä reaaliaikaisen tilannekuvan luomiseksi. Tästä johtuen suurin osa viesteistä lähetetään kryptaamattomina, sillä tiedon saatavuus on järjestelmän toiminnan kannalta luottamuksellisuutta tärkeämpää. [14, s. 2.] Mainittakoon, että 25.5.2018 lähtien Euroopan unionissa jo käytössä olevien sekä tulevien liikennetelemaattisten tietojärjestelmien tulee täyttää tietosuoja-asetus General Data Protection Regulation (GDPR) [21].

Mielenkiintoisena esimerkkinä henkilökohtaisen datan hyödyntämisestä on lähiaikoina hyvinkin julkisesti markkinoitu julkisen liikenteen sovellus ”Whim”, jonka käyttöehdoissa käyttäjä antaa yritykselle vapaat kädet käyttäjästä keräämänsä henkilökohtaisen informaationsa käyttöön ja välittämiseen eteenpäin. Kyseistä sovellusta on markkinoitu hintaan, joka on halvempi kuin HSL:n (Helsingin Seudun Liikenne) kuukausilippu, mutta sisältää kuitenkin isomman skaalan eri palveluita. YLEn tekemän haastattelun mukaan Whimiä pyörittävä Maas Global tekee tappiota kehittääkseen toimintaansa. Myös Toyota ja Veho mainitaan miljoonasijoittajina; datan myymisestä ei tosin mainita sanallakaan. [20]

Henkilökohtaisia tietoja keräävien sovellusten käyttäminen ei kuitenkaan ole pakollista, sillä bussimatkan voi maksaa käteisellä, ainakin toistaiseksi. Ajoneuvojen tapauksessa näin ei välttämättä aina kuitenkaan ole. Yhdysvalloissa liikennevirasto (Department of Transportation, DOT) on aloittanut prosessin, jonka tarkoituksena on tehdä V2X-kommunikaatio pakolliseksi kaikissa uutena myytävissä henkilöautoissa. Väitöskirjassaan Förster summaa tilanteen eurooppalaisesta näkökulmasta seuraavalla tavalla. ”Yksityisyys voikin koitua V2X-järjestelmien kompastuskiveksi: Kansainvälinen Autourheiluliitto (ransk. Fédération Internationale de l'Automobile, FIA) julkaisi hiljattain kyselyn eurooppalaisten kuluttajien mielipiteistä koskien autojen verkottumista. Vastaajista 76 % ilmaisi

kiinnostusta ajoneuvojen verkottumista kohtaan (tärkeimmän osa-alueen ollessa turvallisuus), 88 % vastaajista oli huolissaan henkilökohtaisen datan paljastumisen puolesta, 86 % datan markkinointikäytön puolesta ja 70 % sijainnin seurannan puolesta. Lisäksi 91 % vastaajista halusi verkkoyhteyden olevan katkaistavissa.” [14, s. 3.]

4.3.1 Ajoneuvojen väliset yhteydet

V2V-kommunikaation (ja kaiken muun V2X-kommunikaation) käyttöönoton tarkoituksena on siis liikenteen turvallisuuden ja sujuvuuden parantaminen. Ajoneuvojen välisen kommunikaation, kuten ajoneuvojen sensoridatasta luotujen CAM-viestien vaihtaminen muiden samalla alueella liikkuvien ajoneuvojen kanssa, roolina on varoittaa kuljettajaa esimerkiksi risteävästä liikenteestä tai liikenneruuhkasta. CAM-viestit sisältävät tietoa ajoneuvon sijainnista, nopeudesta ja suunnasta. Näiden viestien sisältämä informaatio mahdollistaa ajoneuvojen tietojärjestelmien liikenteen turvallisuutta ja sujuvuutta tukevien sovellusten käytön.

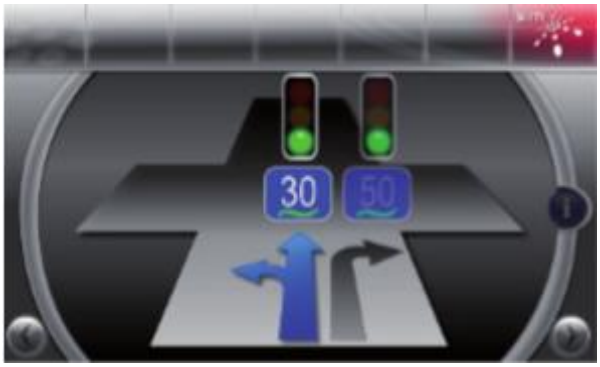
Esimerkkinä tällaisesta sovelluksesta jo edellä mainittu risteävän liikenteen varoitusjärjestelmä ICA (engl. Intersection Collasion Avoidance). Tämän järjestelmän päämääränä on lisätä turvallisuutta risteyksissä. Kuvassa 6 nähdään, kuinka ajoneuvon viihdejärjestelmän välityksellä ICA toimii passiivisena turvajärjestelmänä. Toki itseajavan tai osittain autonomisen ajoneuvon tapauksessa voidaan käyttää auton jarruja tai jopa ohjaus- tai voimansiirtojärjestelmää (täysin autonomisen auton tapauksessa) aktiivisen turvajärjestelmän luomiseksi. [14, s. 12.]

Kuva 6. ICA-järjestelmä, joka varoittaa kuljettajaa risteävästä liikenteestä [14, s. 13].

Toisena esimerkkinä liikenneturvallisuuteen vaikuttavasta sovellutuksesta ruuhkan varoitus. DENM-viestintä (engl. Decentralized Environmental Notification Message) mahdollistaa ruuhkatiedon välittämisen tienkäyttäjälle, joka on vielä kaukana ruuhkasta. Tämän saavuttaminen tosin edellyttää muuta liikennettä: Jos olet kilometrin päässä ruuhkasta ja ajoneuvojen välisen langattoman viestinnän kantama on sata metriä, ei tieto kulje sinulle asti ennen kuin olet jo käytännössä osana ruuhkaa. Mikäli ruuhkan ja sinun välillä kuitenkin on muuta liikennettä, voivat DENM-viestit ”hyppiä” näiden ajoneuvojen kautta sinulle asti ennen ruuhkan saavuttamista. [14, s. 12.] Kuvassa 7 nähdään esimerkki tällaisen järjestelmän kautta tienkäyttäjälle välitetystä ruuhkavaroituksesta.

Kuva 7. DENM-viestinnän kautta välitetty tieto: ruuhkaa 700 metrin päässä [14, s. 13].

Ruuhkavaroitus toimii sekä turvallisuutta että sujuvuutta parantavana tekijänä. Kolmantena esimerkkinä lähinnä sujuvuuteen vaikuttava applikaatio Green Light Optimal Speed Advisory, GLOSA. Tämän ajoneuvojen välisen viestinnän sovelluksen on tarkoitus informoida kuljettajaa tai autonomisen ajamisen järjestelmää optimaalisesta ajonopeudesta liikennevaloihin jäämisen estämiseksi. GLOSAn toiminta perustuu SPaT-viestintään (engl. Signal Phase and Timing), joka tosin vaatii jo viestintää infrastruktuurilta ajoneuvoille, eli liikennevalojärjestelmältä autolle. Kuvassa 7 ajoneuvon viihdejärjestelmän välityksellä saadusta ohjeistuksesta liikenteen sujuvuuden kohentamiseksi. [14, s. 13.]



Kuva 8. GLOSAn välittämä suositus ajonopeudesta liikennevaloihin jäämisen välttämiseksi.

4.3.2 Ajoneuvojen ja tietelematiikan yhteydet

Koska ajoneuvojen ja tietelemaatikan välinen yhteys on tulevaisuuden liikenteen sujumisen ja erityisesti autonomisen ajamisen kannalta ratkaiseva tekijä, on siitä luotava kuluttajille heidän yksityisyytensä lisäksi turvallisuuden kannalta luotettava. Kun jonain päivänä ajoneuvot kulkevat tiellä vain matkustajia kyydissään, täytyy järjestelmän oltava mahdollisimman hyvin suojattu niin ulkoisilta kuin sisäisiltäkin häiriötekijöiltä sekä hyökkäyksiltä. Haasteellisuutta korostaa tarve reaaliaikaiselle datalle, joka puolestaan heikentää käyttäjänsä yksityisyyttä. Järjestelmien kehittäjien yhdeksi suurimmista ongelmista kulminoituu siihen, mitä yksityisyyttä koskevaa informaatiota jaetaan, kenelle ja miten. Esimerkiksi paikkatietojen lähettäminen kryptaamattomana loukkaa käyttäjän yksityisyydensuojaa ja mahdollistaa monia rikollisia aktiviteetteja.

Täysin anonyymin järjestelmän luominen vaatisi suurta määrää laskentatehoa sekä ajoneuvon, että verkoston päässä. Tämä puolestaan johtaa kustannusongelmaan, pelkästään autojen valtavan määrän vuoksi. Kuitenkin turvallisuuden lisääminen liikenteessä säästää valtavan määrän resursseja niin materiaalisella kuin immateriaalisellakin tasolla. Pelkästään Yhdysvalloissa kuoli vuonna 2013 lähes 33 000 ihmistä liikenneonnettomuuksissa. Autojen aktiiviset ja passiiviset turvajärjestelmät ovat toki kehittyneet valtavasti vuosikymmenten aikana, mutta edellä mainittu määrä vastaa noin prosentin sadasosaa Yhdysvaltain väestöstä. Jos vuodessa 1/10 000 ihmisistä kuolee vuosittain liikenneonnettomuuksissa, voidaan todeta kymmenen vuoden aikana yksittäisen henkilön kuolevan liikenneonnettomuudessa todennäköisyydellä 1:1000. Henkien turhan menettämisen lisäksi liikenneonnettomuuksien aiheuttamat kustannukset mitataan kymmenissä miljardeissa euroissa (vuonna 2013 Saksassa 32,5 miljardia euroa). Tähän päälle

arvioitu liikenneruuhkien aiheuttamat kustannukset olivat vuonna 2013 Yhdysvalloissa noin 124 miljardia dollaria ja Saksassa 33,5 miljardia euroa, lisäksi vuoteen 2030 mennessä näiden summien oletetaan kasvavan Yhdysvalloissa 50 %:lla ja Saksassa 31 %:lla. [14, s. 10.]

Pelkästään onnettomuuksien ja ruuhkien aiheuttamien kustannuksien vähentäminen tekee ajoneuvojen ja tietelematiikan verkottumisesta kannattavaa. Lisäpalkintona on myös liikenteen sujuvuuden parantumisen kautta pienenevät hiilidioksidi-, typenoksidi- ja pienhiukkaspäästöt. Yleisen näkemyksen muuttaminen hyväksyväksi V2X-kommunikaation suhteen tietoturvallisuuden takaamisen kautta voi hyvinkin nousta keskeiseen rooliin planeettamme pitämisessä asuinkelpoisena.

Käytännössä tietoturvallinen tiedonsiirto edellyttää ajoneuvon lähettämän datan kryptaamista, ja salausavaimen vaihtamista riittävän usein, jotta ajoneuvon lähettämän paikka- tai muun tiedon lukeminen ei olisi mahdollista. SAE J2945/1 -standardi määrittelee salauksen vaihtoväliksi viisi minuuttia, tosin epäselväksi on jäänyt, miten tähän aikaväliin on päädytty ja onko se riittävä. Väitöskirjassaan Förster tutkii tietokonesimulaation avulla V2X-kommunikaation tietoturvallisuutta. Suojaako J2945/1 -standardin mukainen viestintäprotokolla käyttäjää realistiselta hyökkääjältä, ja kuinka tehokas keino salausavaimen vaihtaminen eri strategioilla on realistisessa liikenneskenaariossa. Kyseinen tutkimus on hyvin yksityiskohtainen, joten sen tarkempi käsittely jätetään tässä työssä tekemättä. Tutkimuksen lopputuloksena Förster toteaa SAE J2945/1 -standardin määrittelemän viiden minuutin salausavaimen vaihtovälin käytännössä täysin riittämättömäksi. Edes kohtuullisen tietoturvallisuuden tason saavuttamiseksi on salausavaimen vaihtovälin oltava noin 45 sekunnin luokkaa. Ajoneuvojen verkottuminen sekä älykkään tiejärjestelmän rakentaminen tietoturvallisuudesta tinkimättä jää haasteeksi. [14, s. 52–53.]

Förster myös pohtii tutkimustyönsä tulosten perusteella, voidaanko hyvää tietoturvallisuuden tasoa saavuttaa, ilman strategioita jotka voisivat vaikuttaa heikentävästi koko järjestelmän tuomaan tieturvallisuuteen. Tietoturvallisuuden saavuttaminen ja yksityisyyden sekä liikenneturvallisuuden takaaminen pysyykin haasteena tulevaisuuden ajoneuvoverkostoratkaisuissa. Saavutettuun tietoturvatasoon vaikuttaa suuresti vallitsevat olosuhteet (kaupunki – maantie, paljon liikennettä – vähän liikennettä). Myös uudelleen määritetyt hyökkäysalgoritmit voivat lisätä seurannan tarkkuutta ja heikentää salauksen

vaihtamisen tuomaa hyötyä tietoturvallisuudessa. Lisäksi salausavainten uudelleenkäyttö nostaa riskiä tilanteelle, jossa hyökkääjä saa selvitettyä tienkäyttäjän kaikki salausavaimet ja voi täten saada hallintaansa kaiken kohteensa liikkumisesta lähetetyn datan. [14, s. 53–54.]

5 Ajoneuvojen tietoturvallisuusuhkia

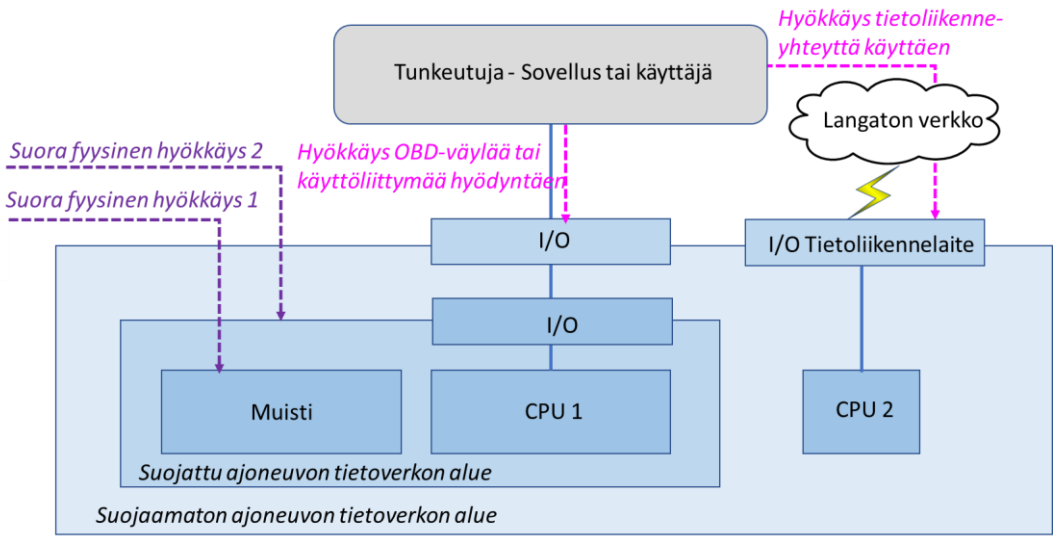
5.1 Taustaa ajoneuvoihin kohdistuvista tietoturvallisuusuhkista

Ajoneuvoihin kohdistuvia tietoturvallisuusuhkia on lukuisia. Hyökkäystavat voidaan karkeasti jakaa kahteen pääluokkaan [9, s. 81] (kuva 9):

1. Suorat fyysiset hyökkäystavat, joissa hyökkääjä pääse suoraan fyysisesti käsiksi ajoneuvon turvallisuuskriittisiin laitteisiin

- Suora fyysinen hyökkäys voi olla tunkeutuva (Invasive, suora fyysinen kontakti esim. muistipiiriin) tai ajoneuvon tietojärjestelmän sisäisiä I/O-rajapintoja hyödyntävä hyökkäys (Non-Invasive)

2. Ulkoisia yhteyksiä hyödyntävät hyökkäystavat (Logical Attack), joissa hyökkäys tapahtuu tietoliikenneprotokollien avulla esim. käyttäen hyväksi ajoneuvon huoltoliittymää (OBD-huoltoväylä), käyttöliittymää tai verkkoyhteyksiä hyödyntämällä.



Kuva 9. Hyökkäystapoja ajoneuvon tietoverkkoon eri rajapintojen kautta

Ajoneuvojen tietoturvallisuusuhkat kohdistuvat eri tavalla riippuen ajoneuvon elinkaaren vaiheesta ja uhkan takana olevan tahon tavoitteista. Esimerkiksi ajoneuvon tai sen osien

valmistajaan kohdistuva uhka voi olla ajoneuvo-ohjelmiston varkaus, joka loukkaa valmistajan teollisia tekijänoikeuksia. Omistajaan kohdistuu esimerkiksi rikollisin keinoin tehty ajonestojärjestelmään murtautuminen ja sitä seuraava autovarkaus. Oman liikenneturvallisuusteen tai ympäristökuormitukseen kohdistuvan uhkaluokkansa muodostaa omistajan toimimesta tai suostumuksella tehtävät ajoneuvon parametri- ja ohjelmistomuutokset. Ne voivat rikkoa valmistajan immateriaalioikeuksia tai takuuehtoja ja muuttaa ajoneuvon ominaisuuksia siten, että ajoneuvo ei täytä takuuehtoja tai katsastusmääräyksiä. Tällaisilla muutoksilla haetaan yleensä auton moottorista lisää tehoa tai vaikutetaan pakokaasujen jälkikäsittelylaitteistoon. Toinen esimerkki sisäisestä uhkasta on ajoneuvon kuljettaja, joka haluaa muuttaa ajotietoja rekisteröivän ajopiirturin tietoja kiertääkseen lainsäätäjän asettamia ajoaikarajoituksia.

Oman tietoturvallisuusuhkaluokkansa muodostavat ajoneuvojen elektronisten ohjaus- ja navigointijärjestelmiin liittyvät ohjelmistovirheet ja suojauksen heikkoudet. Ajoneuvo voi ulkoisten häiriöiden takia toimia virheellisesti (toimilaite toimii väärin) tai esimerkiksi navigointijärjestelmä vie harhaan. Nämä uhkat liittyvät ajoneuvon suunnittelussa tehtyihin järjestelmävalintoihin ja toteutuksen laatuun. Myös ajoneuvon käyttöympäristön olosuhteet voivat muuttua tietoturvallisuutta uhkaaviksi. Esimerkiksi autossa käytetään uuden sukupolven matkapuhelinta, jonka aiheuttamia radiohäiriöitä ajoneuvon elektroniset laitteet eivät siedä.

5.2 Ajoneuvoon kohdistuvia tietoturvallisuusuhkia elinkaaren aikana

5.2.1 Huolto ja ylläpito

Huolto- ja ylläpitohenkilöstö voi anastaa tai luvattomasti luovuttaa kolmansille tahoille ajoneuvon tai valmistajan tietojärjestelmiin tunkeutumisessa tarvittavia tietoturvavälineitä tai tunnisteita. Huoltohenkilöstö voi myös hyödyntää tietoa ajoneuvon virallisista kommunikaatiolaitteista, esimerkiksi väyläviestejä tulkitsemalla, laittomien ohjelmien tai parametrikarttojen asentamiseen ajoneuvon ohjausjärjestelmiin.

Huollon ja ylläpidon henkilöstön voi tarkoituksella tai vahingossa saada pääsyn ja viedä ajoneuvon omistajan tietosuojan piirissä olevia henkilökohtaisia tietoja. Huolto- ja ylläpitotahon tulee käsitellä henkilötietoja EU:n uuden tietosuoja-asetuksen (GDPR) mukaisesti. Huoltoyrityksen täytyy käsitellä rekistereissään olevia asiakastietoja tietosuoja-asetuksen mukaisesti.

5.2.2 Tietoturvallisuusuhkat liikenteessä

Tällä hetkellä liikenteessä oleviin ajoneuvoihin kohdistuvat reaaliaikaiset tietoturvauhkat ovat hyvin vähäisiä. Fyysiset suorat tietoturvahyökkäykset liikkuvaan ajoneuvoon eivät ole käytännössä mahdollisia. Sama tilanne on langallisen huoltoliittymän osalta (OBD). Langattomien, suojaamattomien käyttöliittymien ja verkkoyhteyksien kautta tunkeutuminen on mahdollista. Erityisesti tulevaisuudessa langattomien yhteyksien määrä ajoneuvoihin kasvaa radikaalisti. Kaikki langattomat yhteydet ovat tieto- ja liikenneturvallisuuden kannalta syytä luokitella turvattomiksi, mikäli niitä ei ole suojattu vahvoilla suojausmenetelmillä. Erilaisista suojausmenetelmistä on kerrottu myöhemmin kappaleessa 6.

5.2.3 Käyttäjätietoihin kohdistuvat uhkat

Ajoneuvossa on runsaasti käyttäjäspesifistä, henkilökohtaista tietoa, joka voi päätyä vääriin käsiin. Tällaista tietoa ovat muun muassa ajoneuvon navigointijärjestelmän reittitiedot, viestilaitteiden tunnistetiedot (yhteystiedot jne.), ajonseurantajärjestelmän tiedot. Asiaa on verkottumiseen liittyen käsitelty aikaisemmin kohdassa 4.3.

5.2.4 Varastoinnin ja pysäköinnin tietoturvallisuusuhkat

Kuten johdannossa myös mainittiin, on ajoneuvojen varkaudet muuttuneet ammattimaiseksi liiketoiminnaksi. Nykyjään harvoin otetaan luvatta käyttöön kaksikymmentä vuotta vanha kauppakassi, jotta päästään mukavammin paikasta A paikkaan B, vaan kohteeksi valikoituu mieluummin arvokas premium-auto.

Yhdysvaltain kansallisen liikenneturvallisuushallinnon (National Highway Traffic Safety Administration, NHTSA) on laatinut taulukoita autovarkauksista.

Näissä taulukoissa on suhteutettu varkauksien määrä valmistettujen autojen määrään. Suhteessa kolme eniten varastettua automallia olivat Infiniti Q70 (suhdeluku 6,50 ja listahinta alkaen 51 000 $), Dodge Charger (suhdeluku 4,77 listahinta alkaen n. 30 000 $) ja Infiniti QX70 (4,24 / 47 000 $). Lukumääriltään varastetuimpia autoja olivat kuitenkin yleisimmät käyttöautot, kuten Chevrolet Impala ja Nissan Altima. [18]

Joka tapauksessa vaikka autojen tai oikeastaan mikään tahansa muunkaan vaivalla ansaitun ja hankitun omaisuuden menettäminen rikolliselle taholle on ikävää, on tietoturvallisuuden sovellutuksia nykyään autoissa paljon muuallakin kuin ajon- tai varkaudenestojärjestelmissä. Tietoturvallisuuden haasteet koskevat edellä mainitun lisäksi myös ajoneuvojen ohjelmistopäivityksiä, erilaisissa viihde- ja navigointijärjestelmien funktioita (esimerkiksi matkapuhelimen Bluetooth-yhteys), autojen keräämän datan hallintaa sekä ajoneuvon käyttäjän anonymiteetin suojaamista ja sitä kautta tietosuojalakien noudattamista. [13, s. 5-8]

5.2.5 Uhkien takana olevia tahoja

Ajoneuvojen tietoturvallisuutta uhkaava tahot voidaan jakaa karkeasti kahteen luokaan [9, s. 78]:

- Sisäiset uhkatahot
    - Sisäinen uhkataho voi olla esimerkiksi ajoneuvon omistaja, epärehellinen huoltohenkilö tai autonvalmistajan tehdastyöntekijä
- Ulkoiset uhkatahoja
    - Ulkoisia uhkia muodostavat varkaat, kilpailevat valmistajat, hakkerit, terroristit jne.
    - Ulkoiset sähkömagneettiset häiriöt tai ilmasto-olosuhteet

Oheisessa taulukossa 1 on vertailtu eräitä ajoneuvojen tietoturvallisuutta uhkaavia sisäisiä ja ulkoisia tahoja ja niiden vaikutusta [9, s. 79].

Taulukko 1. Ajoneuvojen tietoturvaa uhkaavia tahoja ja niiden vaikutuksia

	Hyökkääjä S_1 Sisäinen Luokka 1	**Hyökkääjä S_2** Sisäinen Luokka 2	**Hyökkääjä S_3** Sisäinen Luokka 3	**Hyökkääjä U_1** Ulkoinen Luokka 4
Esimerkki hyökkääjästä	Kuski, omistaja	Autoasentajat, takapihamekaanikot	Järjestäytynyt rikollisuus, kilpailijat, tutkijat	Varas, V2I tai V2V ilkivalta
Fyysinen yhteys	Taitotason rajoittama	Kattava, muttei rajaton	Käytännössä rajoittamaton	Olematon tai hyvin rajoittunut
Tekniset resurssit	Yleensä matala	Keskiverrosta korkeaan	Erittäin korkea	Vaihtelee, yleensä matalasta keskitasoon
Tiedolliset resurssit	Yleensä matala	Keskiverrosta korkeaan	Erittäin korkea	Vaihtelee, mutta voi olla korkeakin
Taloudelliset resurssit	Matala	Keskiverto	Erittäin korkea	Yleensä matala
Suojauksen luotettavuus	Pääosin käyttökelpoinen	Vaihtelee, silti käyttökelpoinen	Ainoastaan taloudellisesti	Pääosin käyttökelpoinen

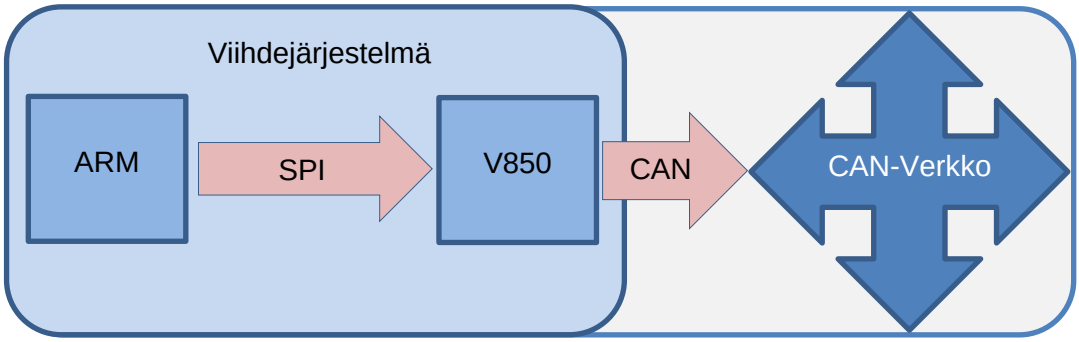
5.3 Esimerkkitapaus Jeep Cherokee 2014

Vuonna 2014 kaksi yhdysvaltalaista ajoneuvoalan tietoturvallisuuden tutkijaa, Charlie Miller ja Chris Valasek, onnistuivat murtautumaan vuosimallin 2014 Jeep Cherokeen sähköiseen ohjausjärjestelmään. Samainen kaksikko oli noin kaksi vuotta aikaisemmin murtautunut myös Toyota Priuksen järjestelmään. Priukseen kohdistuneen hyökkäyksen reaktio ajoneuvovalmistajien suunnalta oli välinpitämätön, haavoittuvuutta pidettiin vähäpätöisenä. Jeepin ja Priuksen tapaukset olivatkin luonteeltaan täysin erilaisia; Kaksikolla oli fyysinen yhteys Priuksen väyläjärjestelmään, kun taas Jeeppiin kohdistuneessa hyökkäyksessä hyödynnettiin auton matkapuhelinverkko- ja Internet-yhteyksiä. Langattomasti tehty hyökkäys johti aivan eri skaalan reaktioon: Jeepin omistava Fiat Chrysler Automobiles (FCA) joutui kutsumaan 1,4 miljoonaa ajoneuvoa päivitettäväksi ajoneuvoteollisuuden historian ensimmäisessä tietoturvallisuuden puutteesta johtuneessa takaisinvedossa. Miller ja Valasek julkaisivat 92-sivuisen raportin tutkimuksestaan vuoden 2014 Black Hat -tietoturvallisuuskonferenssissa Las Vegasissa. [23, s. 4; 24.]

Tämä tapaus onnistuikin herättämään valtavirran ajoneuvojen tietoturvallisuuden heikkouteen. Kyberhyökkääjälle on mahdollista komentaa etänä mitä vain ajoneuvon funktioita, mikrofonin kautta salakuuntelusta auton ohjausfunktioiden (esimerkiksi ohjaus- ja jarrujärjestelmien) manipulointiin. Käytännössä tämä kaksikko pystyi järjestelmän haltuun oton jälkeen komentaa langattomasti tietokoneella mitä tahansa saman heikkouden omaavaa ajoneuvoa koko Pohjois-Amerikan mantereella, kirjaimellisesti omalta kotisohvaltaan. Vuonna 2015 Miller ja Valasek esittelivät Yhdysvaltalaisen tietotekniikkaa käsittelevän WIRED-aikakausilehden toimittajalle, Andy Greenbergille, aikaansaannostaan.

Greenberg lähtee autolla moottoritielle ja Miller sekä Valasek muun muassa sammuttavat moottorin etänä, auton ollessa moottoritiellä Greenberg kyydissään. Tilanne vaikutti melkoisen vaaralliselta ja he esittelevät ominaisuuksia lisää turvallisemmassa ympäristössä. [23, s. 4; 4.]

Charlie Miller ja Chris Valasek hyödynsivät hyökkäyksessään Jeepin viihdejärjestelmästä löytämäänsä tietoturvaheikkoutta. He tutkivat viihdejärjestelmän järjestelmärakennetta ja havaitsivat sitä pyörittävän prosessorin (Texas Instrumentsin 32-bittinen ARM-prosessori) toimivan ”orjana” myös hyvin yleiselle V850-sarjan prosessorille, joka vuorostaan oli yhteydessä CAN-väylään. Viihdejärjestelmän ARM-prosessori ei siis pystynyt komentamaan CAN-väylään yhteydessä ollutta V850-prosessoria, mutta se kuitenkin oli liitettynä tähän SPI-väylän (engl. Serial Peripheral Interface Bus) kautta. Kuva 10 antaa suuntaa rakenteesta. Tämä SRI-väylä oli ratkaisevassa roolissa CAN-viestien lähettämiseksi etänä. Vaikka ARM-prosessori ei suoraan pystynyt lähettämään komentoja, oli kuitenkin mahdollista päivittää V850-prosessorin laiteohjelmisto SPI-väylän kautta. Mainittakoon, että tämän mahdollisti se, ettei V850-prosessoria syystä tai toisesta ollut valmistajan toimesta varmennettu HASH-funktiolla. Miller ja Valasek kirjoittivat V850-prosessorille uuden koodin, jonka ansiosta ARM-prosessorilta SPI-väylää tulevat viestit tulkitaan V850-prosessorissa CAN-komentoina, jotka se lähetti edelleen varsinaiseen CAN-verkkoon. [25]



Kuva 10. Vm. 2014 Jeep Cherokeen viihdejärjestelmän prosessorien väyläliitännät.

Prosessorin uudelleen koodaaminen ei kuitenkaan ole ihan yksinkertainen asia, Millerillä ja Valasekillä siihen kului aikaa yli 3 kuukautta.

Koska uusissa ajoneuvoissa on oltava automaattinen viranomaisten hälytysjärjestelmä onnettomuustilanteita varten, on ajoneuvojen oltava yhteydessä matkapuhelinverkkoon. [30] Tämän yhteyden kautta he onnistuivat viihdejärjestelmän ohjelmiston päivittämisen

jälkeen lähettämään viestejä CAN-väylälle. Matkapuhelinverkon käytön takia he olisivat pystyneet hakkeroitumaan mihin tahansa niistä 1,4 miljoonasta haavoittuvuuden omaavasta ajoneuvosta. Ajoneuvon täysi kontrolloiminen ei kuitenkaan vielä tässä vaiheessa olisi ollut mahdollista. Miller ja Valasek onnistuivat lähettämään viestejä väylälle, mutta aktiivisesti sähköisen ohjainlaitteen (ECU) ohjaamia funktioita, kuten jarrujen tai ohjauksen käyttöä täydestä vauhdista, he eivät pystyneet vielä manipuloimaan. Sen sijaan he hyväksikäyttivät ajoneuvosta jo valmiiksi löytyviä funktioita, kuten automaattista parkkeerausjärjestelmää. Nämä mahdollistivat etähallinnan vain tietyissä tilanteissa, esimerkiksi nopeuden ollessa alle 5 mailia tunnissa tai peruutusvaihteen ollessa päällä. [25; 28.]

Vuonna 2016 WIRED julkaisi uuden artikkelin, joka kertoi tutkijoiden jatkokehittäneen haittaohjelmistoaan. Nyt he kykenivät sulkemaan jonkin auton ECU:ista kokonaan. Tämä tapahtui komentamalla ECU käynnistystilaan (engl. Boot-mode), jota tarvitaan ECU:n uudelleen ohjelmoimiseksi korjaamolla. Oikean ECU:n ollessa hiljaa, he pystyivät estoitta käyttämään sen funktioita väylään liitetyllä tietokoneella, kun taas oikean ECU:n lähettäessä väylälle viestejä samaan aikaan tietokoneen kanssa, väylä tukkeutuu. Tämä tosiaan vaatii fyysisen yhteyden auton CAN-väylään, pelkkä langaton yhteys ei riitä. Lisäksi CAN-väylällä tapahtuvan tietoliikenteen määrän takia on hyvin vaikeaa saada haavoittuvuuden kautta järjestelmää haltuun langattomasti, tai haavoittuvuuden on oltava erityisen vakava. Ohjainlaitteen sulkemisen jälkeen he, väylän liitetyn tietokoneen kautta, pystyivät tekemään käytännössä mitä vain; jarruttamaan, kiihdyttämään tai kääntämään ratin kaakkoon missä tahansa nopeudessa. [28.]

Ottaen huomioon sen, että kyseessä on kahden ihmisen omakustanteisen harrastelun tuloksena löydetty haavoittuvuus, voidaan kuvitella mitä olisi voinut tapahtua, jos haavoittuvuuden olisivat löytäneet paremmin rahoitetut rikollista hyötyä hakevat tahot. Kenties suuremmilla resursseilla olisi voitu jatkokehittää haittaohjelma, joka langattomasti kytkee ohjainlaitteita käynnistystilaan ja ottaa autoja haltuun kesken ajon. Pelkästään mahdollisuus avata 1,4 miljoonan auton ovet takaa rötöstelijälle korkeat tulot. Onneksi haavoittuvuuden löytäneet herrat kuvailevat itseään eettisiksi ihmisiksi, he luonnollisesti ilmoittivat FCA:lle löydöksestään ennen materiaalin julkistamista Internetissä. Jos vastaava mahdollisuus olisi rikollisissa käsissä, voi vain kuvitella mitä kaikkea olisi voinut tapahtua. Todennäköisesti FCA:lle olisi tullut vieläkin isompi lasku kuin ajoneuvojen takaisinkutsusta. Huolestuttavaa on ajoneuvovalmistajan suhtautuminen ongelmiin.

Vuoden 2016 artikkeliin FCA reagoi lähinnä olan kohautuksella, koska fyysisen yhteyden kautta tehtyä hyökkäystä on hyvin vaikea tehdä huomaamatta. Ajoneuvovalmistajien pitäisi aina olla askeleen kyberrikollisia edellä. Miller toteaakin haastattelun päätteeksi: ”Ei ole mitään syytä luulla, että viime vuonna löydetty ja päivitetty bugi olisi ainoa laatuaan. Muissa autoissa todellakin on lisää haavoittuvuuksia, ja todennäköisesti Jeepissä myös.” [25; 28.]

Fiat Chrysler Automobilesin puolesta mainittakoon, että he eivät ole ainoita tietoturvaongelmista jo kärsineistä ajoneuvovalmistajista. Saksan autokerho ADAC (saks. Allgemeiner Deutscher Automobil-Club e.V.) onnistui tutkimuksessaan avaamaan BMW-konsernin (saks. Bayerische Motoren Werke AG) ConnectedDrive-sovelluksella varustettujen ajoneuvojen ovet. Tämä haavoittuvuus koski noin 2,2 miljoonaa BMW-, Mini- ja Rolls Royce -merkkistä henkilöautoa. Se kuitenkin voitiin hoitaa verkon kautta tehdyllä ohjelmistopäivityksellä, ilman takaisinkutsua. Toisessa ADACin tutkimuksessa havaittiin, että 19:sta ajoneuvovalmistajan yhteensä 24:stä eri mallista löydetty haavoittuvuus mahdollisti auton etäavaimen imitoimisen, ovien avaamisen ja auton varastamisen. Tutkimuksessa käytetyn laitteiston arvo oli noin 200 € ja ADACin tutkijan Arnulf Thiemelin mukaan ”laitteiston voi rakentaa jokainen toisen vuoden elektroniikan opiskelija ilman suuria vaikeuksia”. Muutaman mikroprosessorin lisäksi laitteisto vaati vain pariston, radiolähettimen sekä antennin. Lisäksi kiinalaisten tutkijoiden mukaan Teslan Model S -autojen Wi-Fi hotspot mahdollistaa auton järjestelmään tunkeutumisen ja autojen jarrujen etäkäyttämisen jopa 12 kilometrin päästä. [23, s. 5; 13–14; 17.]

6 Ajoneuvojen suojautuminen tietoturvallisuusuhkilta

6.1 Ajoneuvojen suunnittelun tietoturvallisuus

Ajoneuvoihin asennettavien ohjelmistojen suunnittelussa tulee käyttää korkean tietoturvallisuustason suunnittelumenetelmiä ja ympäristöä. Suunnitteluyrityksen tietoverkkoarkkitehtuurin tulisi perustua tietoturvalliseen rakenteeseen, esimerkiksi vyöhykesuojausmalliin (Defence-in-Depth). Suunnitteluyrityksen tietoturvajohtaminen on oltava systemaattista ja tietoturvallisuudelle on asetettava selkeät mitattavat tavoitteet ja niille mittarit sekä toteuttamisesta vastaavat henkilöt. Suunnittelutilojen ja erityisesti tietoturvallisuusmoduulien suunnittelutilojen, fyysinen suojaaminen on oltava korkeatasoinen ja asetetut turvallisuusluokitusnormit täyttävät. [29]

Henkilöturvallisuuteen on panostettava ja kaikille tietoturvallisuuden kannalta tärkeisiin tehtäviin valittaville suunnittelijoille olisi tehtävä turvallisuusselvitys (Security Sreening).

Ajoneuvojen tietoturvallisuuskriittisten moduulien, ohjelmistojen ja sertifikaattien suunnitteluun, hallintaan ja säilytykseen olisi oltava erillinen, tietoturvallisesti kovennettu suunnitteluympäristö työkaluineen, joihin pääsy on rajoitettu vain välttämättömälle henkilöstölle. Työkalujen käyttöä tulee seurata kattavilla lokeilla.

Suunnitteluyhtiön liiketoiminnan riskien- ja jatkuvuudenhallinnan työskentely ja päivittäminen on oltava säännöllistä. Jatkuvuuden hallinnassa on huomioitava laajasti ulkoiset uhkat, muun muassa tietoverkkoihin tunkeutuminen, toimitilaturvallisuus onnettomuuksien varalta, henkilöstöä uhkaavat pandemiat ja terrorismi. [29]

6.1.1 Tietoturvallisuus ajoneuvojen valmistuksessa

Ajoneuvotehdas on tyypillinen prosessiteollisuusympäristö, jonka tietojärjestelmät on suojattava ulkoisia tietoturvallisuusuhkien varalta. Tehdasympäristölle on tyypillistä logistisesti valtavat materiaalivirrat, osien tuonti sekä valmiiden ajoneuvojen pois kuljettaminen. Korkeasta automaatioasteesta huolimatta autotehtaissa työskentelee tuhansia työntekijöitä yleensä useissa vuoroissa.

Tähän tehdasympäristöön on vaikeaa ja kallista rakentaa huipputason tietoturvallisuusympäristö kattavasti, joten ajoneuvojen valmistuksen tietoturvallisuutta vaativat valmistusosuudet, kuten ohjelmistojen, turvallisuusmoduulien ja sertifikaattien asentaminen on keskitettävä sitä varten rakennettuun, eristettyyn ympäristöön. [9]

Ajoneuvovalmistajat käyttävät myös mm. pankki- ja tietotekniikka-aloilla hyödynnettävää käytäntöä, jossa haavoittuvuuksien löytäjille maksetaan palkkioita. Automotive iQ:n e-kirjassa mainitaan, että esimerkiksi FCA maksaa bugin löytäjälle 100 – 1 500 dollaria. Ottaen huomioon, että kyseisen valmistajan autoista löytynyt haavoittuvuus olisi voinut johtaa 1,4 miljoonan ajoneuvon takaisinkutsuakin paljon pahempaan lopputulokseen, tuntuvat summat mitättömiltä. Samaisessa opuksessa mainitaan esim. Teslan maksavan korkeimmillaan 10 000 $ bugin löytäjälle. Samalla mainitaan Teslan palkkalistoilla olevan nelisen kymmentä ajoneuvojen tietoturvallisuuden tutkijaa. Tämä onkin erittäin hyvä asia, kun otetaan huomioon Teslan rooli autonomisen ajamisen edelläkävijänä. Tosin onko määrä riittävä, se jää nähtäväksi. [23, s. 18; 25.]

6.1.2 Ajoneuvojen tietojärjestelmäarkkitehtuuri ja tietoturvallisuus

Ajoneuvojen tietoverkkoarkkitehtuurissa ei ole toistaiseksi panostettu kovin paljon tietoturvallisuuteen. Syitä on monia, esimerkiksi alan perinteikkyys (lue: kehitysprosessien pitkäkestoisuus), pelätään tietoturvaratkaisujen nostavan auton hintaa ja vaikeuttavan huoltoa, tietoturvaratkaisut ovat vieraita autotekniikan suunnitteluinsinööreille, standardoinnin puuttumista jne. Täysin uuden teknologian, vaikka juuri tietoverkkoratkaisun ottaminen käyttöön tuotantoautoissa on myös taloudellisesti hyvin riskialtista. Ajoneuvojen ohjausyksiköiden (ECU) ja -ohjelmistojen peukaloimista rajoittaa hieman teknologian vaativuus. Ohjelmistohakkereiden täytyy hallita suhteellisen vaativa koodaustyö ja heillä täytyy olla käytettävissään ammattimaiset työkalut tehdäkseen muutoksia ajoneuvojen tietojärjestelmiin ja parametrikarttoihin. Lisäksi eri merkkiset ajoneuvot vaativat yleensä omat, valmistajaspesifiset (ECU spesifiset) laitteet ohjausyksiköiden ohjelma- ja parametrikoodin lukemiseksi tai muuttamiseksi. Osaavalle ostajalle markkinoilta on kuitenkin vapaasti saatavana laaja valikoima erilaisia ohjelmointi- ja diagnosointilaitteita sekä ohjelmia, joilla päästään peukaloimaan ajoneuvojen parametrikarttoja ja ohjausohjelmia. Tästä syystä ajoneuvojen perinteiset tietojärjestelmät ovat haavoittuvia ja mahdollistavat ajoneuvoihin kohdistuvia tietoturvarikkomuksia, joista esimerkkejä lueteltiin luvussa 5.

Tietoturvalliselle järjestelmäarkkitehtuurille on ominaista, että sen muodostaa vain luotetut (tunnistetut) ja sertifioidut ohjausyksiköt, sensorit, sovellusohjelmat ja tietoturvaohjelmistot sekä -mekanismit. Tietoteknistenlaitteiden tunnistamiseen IP-pohjaisissa tietoverkoissa on useita erilaisia standardisoituja menetelmiä ja protokollia. Näistä yksi pisimpään käytetty on ollut MAC-osoitteeseen (Media Access Control) perustuva laitetunnistaminen. Vastaavanlaisia ”osatunnistuskoodeja” on käytetty myös ajoneuvoteollisuudessa vaihtelevalla menestyksellä. Valitettavasti osatunnisteet ovat yleensä olleet salaamattomia, jolloin ne on ollut helppo kiertää. [9, s. 123.] Toisaalta kiinteisiin tietoverkkoihin kehitetyt modernit ja hyvin tietoturvalliset tunnistusmenetelmät vaativat runsaasti prosessointikapasiteettia ja soveltuvat huonosti reaaliaikaiseen automaatioympäristöön, jollainen ajoneuvoympäristökin on. Laite- ja ohjelmistotunnisteiden ja sertifikaattien täytyy olla ajoneuvokohtaisia, jotta tietomurron sattuessa vahingot olisivat mahdollisimman rajattuja. Salausalgoritmeihin perustuvilla ja fyysisesti kopioimattomilla menetelmillä (PUF, Physically Unclonable Function) on mahdollista tunnistaa ja yksilöidä ajoneuvon osat/laitteet ja ohjelmat tietoturvallisesti tiettyyn ajoneuvoon kuuluviksi. [9, s. 123, 124.]

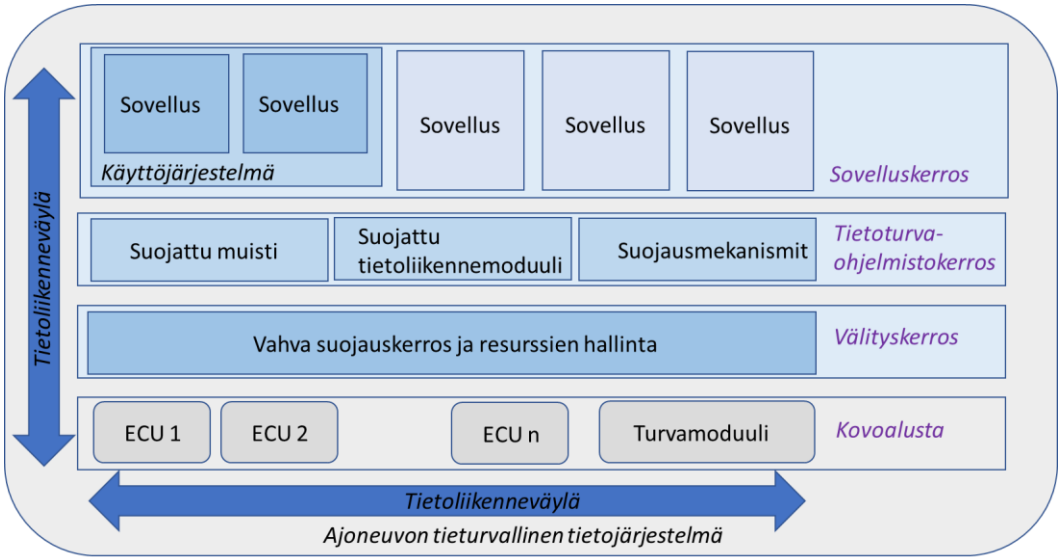
Ohjelmiston kehittämisessä ja toteutuksessa on käytettävä tietoturvallisia suunnittelumenetelmiä ja estettävä vakiohaavoittuvuuksien esiintyminen [9, s. 128–131].

Wolf on lähteen [9] luvuissa 7 ja 8 käsitellyt ja vertaillut tietoturvallisen ajoneuvoympäristön erilaisia (tietoturva)vaatimuksia ja suojausmenetelmiä. Näistä mainittakoon seuraavat ominaisuudet ja vaatimukset:

- peukaloinnin tunnistaminen, reagointi, sietäminen ja estäminen
- ajoneuvojen varustaminen tietoturvallisuusmoduuleilla
- ajoneuvojen varustaminen tietoturvaohjelmilla ja -ohjelmamoduuleilla
- digitaalisten allekirjoitusten ja turvasirujen käyttäminen
- luotettujen järjestelmäalustojen käyttäminen (TPM, Trusted Platform Module)
- käyttäjien luotettava autentikointi.

Kuvassa 7 on esitetty ehdotus Wolfin malliin perustuvasta ajoneuvon tietoturvallisesta järjestelmäarkkitehtuurista. Siinä laitealusta perustuu perinteisestä ajoneuvoissa käytetystä laitealustasta lisättynä mikropiiripohjaisella turvamoduulilla.

Turvamoduulilla toteutetaan kriittisen tietoturvaoperaatiot, kuten esim. salaus, koodaus ja tarkistetiivisteiden laskenta. Suojakerros mahdollistaa laitealustan ja käyttöjärjestelmän sekä sovellusten eristämisen toisistaan. Suojakerros voidaan toteuttaa esimerkiksi perinteisillä ajoneuvoissa käytetyillä kompakteilla käyttöjärjestelmillä tai mikrokerneliin perustuvilla ratkaisuilla. Tietoturvaohjelmistokerroksella toteutetaan turvallinen tiedon varastointi ja tietoliikenne. Ylimmällä tasolla sijaitsevat varsinaiset ajoneuvotekniset sovellukset [9, s. 136–138.]



Kuva 7. Ehdotus ajoneuvon tietoturvallisesta järjestelmäarkkitehtuurista [9, s. 137].

Yksi mahdollisuus tietoturvallisen järjestelmäarkkitehtuurin toteuttamiseksi on käyttää erityistä suojattua laitealustaa (hardware isolation). Tällaisia laitealustoja tarjoavat esimekiksi ARM ja Intel, [9, s. 139-140].

6.1.3 Laitteiden ja ohjelmistojen tietoturvallinen identifiointi

Tällä hetkellä ajoneuvoon asennettavia ohjelmistojen ja varaosien aitous tarkistetaan vain poikkeuksellisesti ajoneuvon tietojärjestelmän toimesta. Ohjelmistoille ja parametrikartoille tehdään virheentarkistuksia tarkistussummienavulla, mutta ohjelmistojen ja parametrikarttojen aitoutta ei vahvisteta virallisilla sertifikaateilla. Tarkistussummat ovat valistuneen hakkerin helposti uudelleen laskettavissa, sillä tiivistealgoritmit ovat yleisesti tunnettuja [9, s. 133].

Tämä mahdollistaa osaaville henkilöille ja korjauspajoille ajoneuvojen virittämisen sekä ohjelmistojen, että mekaanisten rakenteiden osalta. Varaosahinnat pysyvät tietysti kohtuullisina, kun käytettävissä on halpoja korvikevaraosia. Tämä lienee toivottavaa kalliin autoilun maassa, kuten Suomessa.

Haluttaessa pitää ajoneuvon tietojärjestelmäympäristö tiukasti valmistajan ja viranomaisten vaatimusten mukaisena, edellytetään ajoneuvon huoltoväylään liitettävien huoltolaitteiden ja ajoneuvoon asennettavien ohjelmistojen, parametrikarttojen ja varaosien luotettavaa tunnistamista. Luotettava tunnistaminen voidaan tehdä esimerkiksi digitaalisten allekirjoitusten tai vastaavien luotettujen sertifikaattien avulla [9, s. 134]. Ohjelmistojen ja parametrikarttojen tunnistaminen luotetuiksi ja virheettömiksi tulisi tehdä sekä niitä ladattaessa ajoneuvon tietojärjestelmään että ajoneuvoa käynnistettäessä tietojärjestelmän alustuksen yhteydessä.

Toinen ja tietoturvamielessä erittäin vahva vaihtoehto on käyttää eritystä laitepohjaista aitoussertifiointia. Ratkaisu on tehokas, mutta kallis ja hankaloittaa ohjelmistojen päivittämistä. Yksi mahdollisuus on käyttää luotettua tietojärjestelmäalustaa, jossa vahva tunnistaminen perustuu HASH-algoritmien ja turvasirun yhteiskäyttöön. [9, s. 135.]

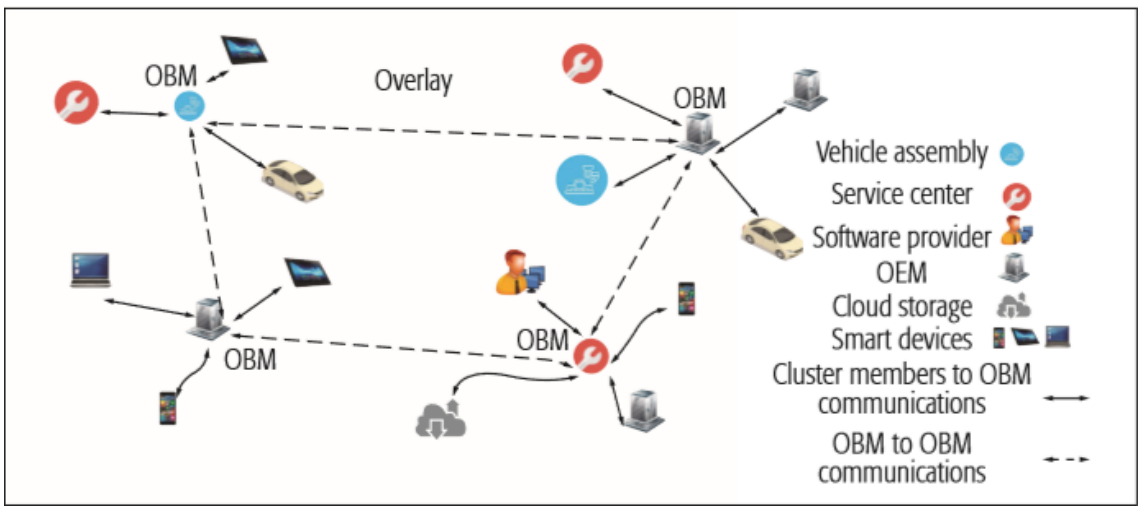
Vahvimmassa muodossaan ajoneuvon ohjelmiston tulisi asettua lukittuun suojatilaan, mikäli tietoteknistä ympäristöä hallinnoiva kontrolliyksikkö havaitsee sertifioimattomia huoltolaitteita, ohjelmistoja tai varaosia.

6.1.4 Esimerkkejä ajoneuvojen tietoturvallisista järjestelmäratkaisuista

Täysin tietoturvallista järjestelmäratkaisua ei ole olemassa. Tämä ei kuitenkaan tarkoita sitä, etteikö tietoturvallisuuteen pidä panostaa. Mielenkiintoisin ”uusi” tietoturvallinen toimintamalli on Bitcoinien kautta yleiseen tietoisuuteen noussut lohkoketjutekniikka (engl. Block Chain, BC). Lohkoketju perustuu julkisen avaimen salaukseen, jokaisella käyttäjällä on kaikkien käytettävissä oleva julkinen avain. Jokaisella käyttäjällä on lisäksi salainen avain, joka on tallessa hänen henkilökohtaisella laitteellaan. Bitcoinin tapauksessa jokainen transaktio tallentuu järjestelmän jokaiseen verkoston solmuun, jolloin yhtä kolikkoa ei voi käyttää kahteen kertaan. Käyttäjät voivat nähdä transaktion tapahtuneen, mutteivat tiedä sen osallisia. Tallennettu informaatio kootaan kronologisessa järjestyksessä ryhmiksi (lohkoiksi), jotka muodostavat lohkoketjun. Matemaattisen prosessin ansiosta yksittäisen käyttäjän on erittäin vaikeaa saada lohkoketjun kaapattua.

Bitcoin on herättänyt paljon keskustelua ja negatiivistakin palautetta: sen katsotaan olevan viranomaiskontrollin puutteen takia lähinnä rikolliseen kaupankäyntiin ja rahoitukseen tarkoitettu valuutta. Lisäksi yhtenä validina argumenttina mainittakoon, että Bitcoinin lohkoketjujen ylläpito kuluttaa tällä hetkellä saman verran sähköä kuin yli 10 miljoonan asukkaan Tšekin tasavalta. [26; 27.]

Lohkoketjuja ja ajoneuvoja käsiteltiin IEEE Communications Magazinen joulukuun 2017 painoksessa. Artikkelin mukaan nykyiset kommunikaatio arkkitehtuurit eivät huomioi käyttäjänsä yksityisyyttä. Autonomisen ajamisen sovellusten yleistyessä voisi järjestelmän kaatuminen aiheuttaa vakavia seuraamuksia. Älykkäät ajoneuvot, niiden valmistajat ja tulevaisuudessa muut autonomisen ajamisen osat (esim. tietelematiikka) muodostavat eräänlaisen rajapinnan, jossa ne kommunikoivat toistensa kanssa. Lohkoketjun solmukohdissa datan säilyttäminen poistaa tarpeen tällaiselle tietoturvallisuusriskinä nähtävälle ajoneuvojen, valmistajien ja infrastruktuurin rajapinnalle. Kuvassa 11 nähdään lohkoketjuun perustuva ajoneuvojen verkostorakenne. Lisäksi lohkoketjuissa tiedon ”pirstaloitunut” luonne tekee yksittäisen käyttäjän tietojen kalastelusta käytännössä mahdotonta, ilman tämän symmetrisen avaimen murtamista (esimerkiksi AES-standardin mukaista kryptausta pidetään yleisesti hyvin turvallisena). Kirjoittajien mielestä lohkoketjuteknologia voi olla hyödyllinen ajoneuvosovellutuksissa. ”Lohkoketjun esittelemä vahva kommunikaatioturvallisuus ja tunnistautuminen lieventävät riskiä ajoneuvon etähakkerointiin ja täten kohentaa matkustajien turvallisuutta”. [15, s. 1-2.]



Kuva 11. Lohkoketjuun perustuva ajoneuvojen, autovalmistajien, pilvipalveluiden ja muiden laitteiden verkko [15, s. 5].

Artikkelissa mainitaan lohkoketjujen parantavan ajoneuvon tietoturvallisuuden ohella myös ajoneuvoihin liittyvien palveluiden tietoturvaa. Mainittuja palveluita ovat muun muassa vakuutukset (tulevaisuudessa vakuutusyhtiö todennäköisesti räätälöi maksuja asiakkaiden mukaan), sähköautojen lataus (latauksessa liikkuva data vaarantaa käyttäjänsä yksityisyyden), autojen jakamispalvelut (yksityisyyttä tukeva maksu- ja vuokraustapahtuma) sekä autojen valmistajien kautta (engl. Original Equipment Manufacturer, OEM) ladattavat ohjelmistopäivitykset. Artikkelin päätteeksi sen kirjoittajat ehdottavat uutta ajoneuvoteollista tietoturvallista arkkitehtuuria, joka vähentää tarvetta keskitetylle hallinnalle ja mahdollistaa uusia ajoneuvoihin liittyviä liiketoiminnan malleja. [15, s. 6–7.]

Energiayhtiö Fortum Oyj on testannut lohkokooditekniikan toimivuutta myös sähkökaupan transaktioiden todentamisessa [29].

6.2 Huollon ja ylläpidon tietoturvallisuus

6.2.1 Huoltojärjestelmien ja -toimintaympäristön tietoturvallisuus

Ajoneuvojen huoltoa ja ylläpitoa suorittavat pienyritykset ovat merkittäviä toteuttajia sertifioimattomien ohjelmistojen, varaosien asentamisessa sekä ajoneuvojen virittämisessä. Tietoturvallisen huoltoympäristön luominen edellyttää huoltoliikkeeltä sitoutumista laitevalmistajan ja maahantuojan tietoturvakäytäntöihin ja -sääntöihin. Tämä voidaan toteuttaa esimerkiksi sanktioidun tietoturvallisuussopimuksen muodossa. Sopimuksessa voidaan määrittää ne huoltojärjestelmät, varaosat, ohjelmistolähteet ja työmenetelmät, joita valtuutettu huoltoliike sitoutuu käyttämään tietoturvavaatimukset täyttääkseen. Lisäksi tietoturvakriittiseen aineistoon pääseviltä henkilöiltä voidaan vaatia henkilökohtaista tietoturvasitoumusta. [29]

6.2.2 Tietoturvallinen ohjelmistojen päivittäminen

Wolf esittää kaksi menetelmää ajoneuvo-ohjelmistojen tietoturvalliseksi päivittämiseksi [9, s. 141–145]. Ne perustuvat joko digitaalisiin allekirjoituksiin tai luotetun tietojärjestelmäalustan (Trusted Computing) käyttöön. Ensi mainitussa ajoneuvoihin asennetaan vain valmistajan digitaalisella allekirjoituksella (sertifikaatilla) varustettuja ohjelmistoja.

Luotetussa tietojärjestelmäratkaisussa laitevalmistaja voi sitoa jaettavat ohjelmistopäivitykset tiettyyn ajoneuvoon ja laite- ja ohjelmistoympäristöön kuuluviksi. Päivitykset on suojattu vahvoin tietoturva-algoritmein, ja ne toimivat vain kyseisessä ajoneuvossa.

6.3 Tietoturvallisuus liikenteessä

Liikenneturvallisuutta tieliikenteessä voidaan parantaa käyttämällä aktiivisilla turvallisuusominaisuuksilla varustettuja ajoneuvoja, rakentamalla liikenneturvallisuutta lisääviä telemaattisia turvajärjestelmiä sekä muokkaamalla ihmisten asenteita. Ajoneuvojen ja tieinfrastruktuurin kehittäminen vie runsaasti aikaa ja vaatii suuria pääomia varsinkin, jos halutaan kehittää ajoneuvoja itseohjautuviksi laitteiksi. Itseohjautuvien ajoneuvojen ja älykkään tietelematiikan odotetaan parantavan huomattavasti liikenneturvallisuutta, toimiakseen ne vaativat ehdottoman luotettavaa tietotekniikkaa ajoneuvoissa sekä varmaa tiedonsiirtoa. Niiden kehittäminen vaatii oman aikansa ja mahdollisesti myös viranomaisten ohjaavaa sääntelyä. Esimerkkinä teknologian läpimurtoon vaadittavasta ajasta on sähköautoiluun siirtyminen. Laajamittainen täyssähköautoihin siirtyminen harvaan asutussa maassa, kuten Suomessa, vaatii sekä teknologisia läpimurtoja (akkuteknologia) että isoja investointeja latausinfrastruktuurin kehittämiseen. Todennäköisesti ajoneuvoteknologian kehitys tulevaisuudessa pohjautuu pieniin jatkuviin parannuksiin sekä ajoneuvoteknologian että turvallisuustekniikan osalta. Suuria vallankumouksellisia kertamullistuksia tuskin on odotettavissa.

6.4 Ajoneuvovarkauksilta suojautuminen

Ajoneuvovarkaudet muodostavat merkittävän talousrikollisuuden muodon kuten kohdassa 5.2.4 todettiin. Elektronisten ajonestojärjestelmien ja sähköisten lukitusjärjestelmien yleistyttyä ajoneuvovarkaudet vaativat erikoislaitteiden käyttämistä ja varkaudet ovat muuttuneet ammattimaisiksi. Ajoneuvovarkauksilla haetaan lähes poikkeuksetta taloudellisia hyötyjä ja varastettujen ajoneuvojen alkuperä pyritään hävittämään ja myymään ajoneuvot uusiin kohdemaihin.

Elektronisten suojausjärjestelmien parantamiseksi tulisi esimerkiksi siirtyä kertakäyttöisiin salasanoihin sekä ajoneuvon lukituksessa että ajonestojärjestelmän deaktivoinnissa.

Tällä estettäisiin ”salakuuntelulaitteiden” käyttäminen autojen elektronisten lukitusjärjestelmien murtamisessa, [29]. Lohkokooditekniikka on myös yksi, uusi ja lupaava teknologia, jolla voitaisiin parantaa ajoneuvojen lukitusjärjestelmien tietoturvallisuutta (lisätietoja kohdassa 6.1.4).

Ajoneuvojen varkauksia voidaan vähentää myös säilyttämällä niitä fyysisesti hyvin suojatussa ympäristössä. Myös ajoneuvon avaimia tulisi säilyttää huolellisesti, esimerkiksi ”keyless entry” -tyyppisiä avaimia voisi säilyttää RFID-suojatussa pussukassa (engl. Radio Frequency Identification). Autotalleihin ja vastaaviin varastotiloihin tulisi olla pääsy vain siihen valtuutetuilla henkilöillä. Kulkuoikeudet ja niiden hallinnointi tulisi toteuttaa tietoturvallisilla elektronisilla menetelmillä. Kaikkia kulkutapahtumia ajoneuvojen säilytystiloihin voi silloin seurata kulunvalvontajärjestelmän lokista. Tarve seurannalle kasvaa yhteiskäyttöautojen lisääntyvän suosion myötä. [29]

7 Yhteenveto

Insinöörityö aloitettiin käymällä ohjaajan kanssa läpi aihealue ja työn luonteen asettamat vaatimukset. Todettiin, että tiedonhaku on selvityksen onnistumisen kannalta ensiarvoisen tärkeää. Tiedonhaku aloitettiin heti aiheen hyväksymisen jälkeen, ja se jatkui aina kirjoitusvaiheen loppuun saakka. Esimerkiksi väitöskirjoja lukiessa tehtiin muistiinpanoja, joita pyrittiin vertaamaan muista lähteistä löydettyyn tietoon ja sitä kautta varmistamaan käytetyn tiedon luotettavuus sekä ajankohtaisuus.

Selvitystyön perusteella vaikuttaisi siltä, että tuotteidensa tietoturva-asioissa ajoneuvovalmistajat luottavat paljon fyysiseen suojaukseen, ehkä liiaksikin. Ajoneuvojen sisäiset tietoväylät, joissa turvallisuuskriittisin tieto kulkee, ovat hyvin suojattuina ulkoisilta uhilta auton rakenteiden sisällä. Lisäksi väylällä tapahtuvan tiedonsiirron suuresta määrästä johtuen, on langattomien hyökkäysten hyvin vaikea saavuttaa kontrollia järjestelmässä. Ajoneuvoteollisuudessa käytetään kuitenkin hyvin paljon alihankkijoiden tuottamia järjestelmiä, joita hyödynnetään laajasti eri automalleissa ja -merkeissä. Alihankkijan toimittamasta osakokoonpanosta, esimerkiksi viihdejärjestelmästä, löytyvä haavoittuvuus voikin aiheuttaa vakavan tietoturvallisuusriskin. Perimmäinen kysymys tässä on tietysti rahasta. Ajoneuvonvalmistaja hyödyntää yhtä komponenttia tai järjestelmää mahdollisimman monessa eri kohteessa säästääkseen rahaa. Komponenttivalmistaja ei välttämättä kiinnitä huomiota valmistamiensa komponenttien tietoturvallisuuteen, vaikkapa jos tietoturvallisuutta ei tuotesuunnitteluprosessin vaatimusmäärittelyssä ole tuotu esille. Toisaalta kalliiden mallikohtaisten ratkaisujen käyttämiseen on suuri kynnys alalla, jossa toimijoita on monia ja kilpailu on kovaa.

Langattomia haavoittuvuuksia pidetään kasvavana riskinä ajoneuvon käyttäjälle. Fyysiseen väylään liittyminen on vaivalloista ja hyvin vaikeaa tehdä huomaamatta. Langaton isku sen sijaan voi tapahtua missä vain, milloin vain. Langattomasti suoritettavaa hienostunutta hyökkäystä on myös vaikea tunnistaa, sillä sen onnistuminen on sidottu sen havaitsemattomuuteen. Erityisesti itseajavissa ajoneuvoissa vakavimpana uhkakuvana on ajoneuvon käytön estäminen, mahdollisesti jopa sen haltuunotto kesken ajon. Yleisen liikenneturvallisuuden lisäksi langattomien ratkaisujen yleistyminen heikentää käyttäjän yksityisyyttä. Langattomien hyökkäysten kautta on myös mahdollista selvittää tietoja käyttäjästä, ja käyttää näitä kiristämiseen tai muuhun rikolliseen toimintaan. Jo ilmi tulleet haavoittuvuudet ovat onneksi tapahtuneet pääasiassa rehellisten tutkijoiden toimesta, jolloin ajoneuvoteollisuus sekä käyttäjäkunta ovat tulleet tietoisiksi ongelmasta. Voidaan

kuitenkin olla varmoja ajoneuvojen vielä tuntemattomien haavoittuvuuksien olemassa olosta, ja siitä että jossain suunnitellaan tälläkin hetkellä uutta haittaohjelmaa rikollisiin tarkoituksiin. Ajoneuvovalmistajien ja muiden alan toimijoiden on jatkossa kehitettävä tietojärjestelmiään tietoturvallisuus joukon kärjessä. Joka tapauksessa ajoneuvojen kehittyessä yhä monimutkaisemmiksi tietojärjestelmiksi, ovat tietoturvallisuus- sekä autoalat löytäneet toisensa ja se on meidän kaikkien kannalta hyvä asia.

Hakkeroinnin riskien minimoimiseksi ajoneuvoteknisten tietojärjestelmien rakennetta on kehitettävä muiden turvallisuuskriittisten järjestelmien suuntaan. On käytettävä rakenteellisia rajapintoja tietojärjestelmien arkkitehtuurissa sekä varsinaisia suojausjärjestelmiä tietoturvallisuuden takaamiseen. Ajoneuvojen suunnittelussa pitäisi hyödyntää tietoturva-alan ammattilaisten taitoja mahdollisimman paljon haavoittuvuuksien löytämiseksi. Tulevaisuudessa ajoneuvojen keskinäisen sekä liikenteenohjauksen välisen tietoliikenteen toteuttaminen tietoturvallisesti on yksi alan suurimmista haasteista. Standardisointia on syytä kehittää, mutta toisaalta olisi vältettävä rakenteeltaan identtisten järjestelmärakenteiden käyttöä laajasti. Saatavilla on kuitenkin jo uutta teknologiaa, jonka hyödyntämiseen ajoneuvoteknisissä tietojärjestelmissä ajoneuvovalmistajat toivottavasti perehtyvät.

Vaikka haittaohjelmia ei ajoneuvoissa ole vielä juurikaan nähty, on varmaa tai ainakin hyvin todennäköistä, että niitä tullaan vielä näkemään. Ajoneuvoon kohdistuvan kyberhyökkäyksen vaikutus käyttäjään voi olla täysin erilainen perinteisiin tietoverkkojen kautta tehtäviin hyökkäyksiin verrattuna: Auton tilanteessa on hyökkäyksen uhri mahdollisesti vakavassa fyysisessä vaarassa. Tietosuojaa ja yksityisyyttä kuitenkaan unohtamatta. Massavalvonnan, virtuaalirahan ja haittaohjelmien kautta kiristämisen aikakautena lainaan lopuksi NSA:n tietovuotajana tunnetuksi tullutta Edward Snowdenia: ”Arguing that you don’t care about the right to privacy because you have nothing to hide is no different than saying you don’t care about free speech because you have nothing to say” [14, s. 14].

Lähteet

1 Zwass, V. 2011. Information System. Verkkoaineisto. Encyclopædia Britannica. <https://www.britannica.com/topic/information-system>. Luettu 27.3.2018.

2 U.S. Code, Title 44, Chapter 35, Subchapter III, § 3542.

3 James, S. 2018. What is Information Security? Verkkoaineisto. ISMS.online. <https://www.isms.online/vocabulary/information-security-2/>. Luettu 28.3.2018.

4 ISMS.online. 2018. CIA Triad of Information Security. Verkkoaineisto. <https://www.isms.online/?s=Information+Security>. Luettu 28.3.2018.

5 Cherdantseva, Y. & Hilton, J. 2013. Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals. Teoksessa Almeida, F. & Portela, I. (toim.): Organizational, Legal, and Technological Dimensions of Information System Administrator. Hershey, Pennsylvania: IGI Global Publishing.

6 Hosch, W.L. 2009. Firewall. Verkkoaineisto. Encyclopædia Britannica. <https://www.britannica.com/technology/firewall>. Luettu 28.3.2018.

7 The Government of the Hong Kong Special Administrative Region. 2008. Verkkoaineisto. Hong Kongin erityishallintoalueen hallitus. <https://www.infosec.gov.hk/english/technical/files/vulnerability.pdf>. Luettu 28.3.2018.

8 Simmons, G. J. 1999. Cryptology. Verkkoaineisto. Encyclopædia Britannica. <https://www.britannica.com/topic/cryptology>. Luettu 28.3.2018.

9 Wolf, M. 2008. Security Engineering for Vehicular IT Systems. Improving the Trustworthiness and Dependability of Automotive IT Applications. Dissertation. Ruhr-Universität Bochum.

10 Simmons, G.J. 2009. Data Encryption Standard. Verkkoaineisto. Encyclopædia Britannica. <https://www.britannica.com/topic/Data-Encryption-Standard>. Luettu 28.3.2018.

11 Simmons, G.J. 2009. Advanced Encryption Standard. Verkkoaineisto. Encyclopædia Britannica. <https://www.britannica.com/topic/AES>. Luettu 28.3.2018.

12 National Institute of Standards and Technology. 2008. Federal Information Processing Standards Publication 197. Announcing the ADVANCED ENCRYPTION STANDARD (AES). Verkkoaineisto. <https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf>. Luettu 28.3.2018.

13 Lemke, K.; Paar, C. & Wolf, M. 2006. Embedded Security in Cars. Securing Current and Future Automotive IT Applications. eBook. Berliini: Springer.

14 Förster, D. 2016. Verifiable Privacy Protection for Vehicular Communication Systems. Dissertation. Ulm University.

15 Dorri, A.: Steger, M.: Kanhere, S.S. & Jurdak, R. 2017. BlockChain: A Distributed Solution to Automotive Security and Privacy. IEEE Communications Magazine December 2017. s. 119–125.

16 ISO/SAE AWI 21434. Road Vehicles – Cybersecurity engineering. International Organization for Standardization, Society of Automotive Engineers. Kehitteillä oleva standardi. <https://www.iso.org/standard/70918.html>. Luettu 28.3.2018.

17 About AUTOSAR. Verkkoaineisto. AUTOSAR. <https://www.autosar.org>. Luettu 28.3.2018.

18 NHTSA. Theft Database. Internet-tietokanta. <https://one.nhtsa.gov/apps/jsp/theft/index.htm>. Luettu 1.5.2018.

19 SAE J3061_201601. Cybersecurity Guidebook for Cyber-Physical Vehicle Systems. <https://www.sae.org/standards/content/j3061_201601/>. USA: Society of Automotive Engineers.

20 Salminen, R. 2017. Mikä ihmeen Whim? – Uusi palvelu yhdistää bussit, taksit, kaupunkipyörät ja vuokra-autot yhden klikkauksen alle, mutta väheneekö yksityisautoilu? Verkkoaineisto. YLE Uutiset. <https://yle.fi/uutiset/3-10171507>. Luettu 3.5.2018.

21 SAE J2945/1_201603. On-Board System Requirements for V2V Safety Communications. <https://www.sae.org/standards/content/j2945/1_201603/>. USA: Society of Automotive Engineers.

22 Tietosuojavaltuutetun toimisto. 2015. EU:n tietosuojauudistus. Verkkoaineisto. <http://www.tietosuoja.fi/fi/index/euntietosuojauudistus.html>. Luettu 3.5.2018.

23 AUTOMOTIVE CYBER SECURITY – Dedicated eBook for the Cyber Security professional. 2017. Verkkoaineisto. Automotive IQ. <https://www.automotive-iq.com/iqpc-landing-page/automotive-cyber-security-complete-ebook>. Luettu 28.3.2018.

24 WIRED. 2015. Hackers Remotely Kill a Jeep on the Highway – With Me in It. Verkkoaineisto. YouTube. <https://www.youtube.com/watch?v=MK0SrxBC1xs>.

25 DEFCONConference. 2015. DEF CON 23 - Charlie Miller & Chris Valasek - Remote Exploitation of an Unaltered Passenger Vehicle. Verkkoaineisto. Youtube. <https://www.youtube.com/watch?v=OobLb1McxnI>.

26 Digiconomist. 2018. Bitcoin Energy Consumpiton Index. Verkkoaineisto. <https://digiconomist.net/bitcoin-energy-consumption>. Luettu 4.5.2018.

27 Gregersen, E. 2012. Bitcoin. Verkkoaineisto. Encyclopædia Britannica. <https://www.britannica.com/topic/Bitcoin>. Luettu 6.5.2018.

28 Greenberg, A. 2016. The Jeep hackers are back to prove car hacking can get much worse. Verkkoaineisto. WIRED. <https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/>. Luettu 6.5.2018.

29 Tervo, Jouko. 2018. Konsultti, Reneco Oy. Helsinki. Suullinen haastattelu. 20.4.2018.

30 Euroopan komissio. 2015. eCall in all new cars from April 2018. Verkkoaineisto. <https://ec.europa.eu/digital-single-market/en/news/ecall-all-new-cars-april-2018>. Luettu 6.5.2018.