Analiza potencijalnih točaka za neovlašteni pristup povezanim vozilima

Marinčević, Ivan

Master's thesis / Diplomski rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:119:154255

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Ivan Marinčević

ANALIZA POTENCIJALNIH TOČAKA ZA NEOVLAŠTENI PRISTUP POVEZANIM VOZILIMA

DIPLOMSKI RAD

Zagreb, rujan 2022.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 25. ožujka 2022.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Forenzička analiza informacijsko komunikacijskog sustava**

DIPLOMSKI ZADATAK br. 6697

Pristupnik: **Ivan Marinčević (0135227468)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Analiza potencijalnih točaka za neovlašteni pristup povezanim vozilima**

Opis zadatka:

Objasniti koncept povezanih vozila. Definirati arhitekturu i komunikacijske tehnologije povezanih vozila. Odrediti elemente i mehanizme za neovlašteni pristup povezanim vozilima. Prikazati motivaciju i instrumente za neovlaštene pristupe u povezanim vozilima. Analizirati mogućnosti forenzičke analize povezanih vozila.

Mentor:

doc. dr. sc. Siniša Husnjak

Predsjednik povjerenstva za diplomski ispit:

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

DIPLOMSKI RAD

ANALIZA POTENCIJALNIH TOČAKA ZA NEOVLAŠTENI PRISTUP POVEZANIM VOZILIMA

ANALYSIS OF THE POTENTIONAL POINTS OF UNAUTHORIZED ACCESS TO CONNECTED VEHICLES

Mentor: doc.dr.sc. Siniša Husnjak

Student: Ivan Marinčević

JMBAG: 0135227468

Zagreb, rujan 2022.

ANALIZA POTENCIJALNIH TOČAKA ZA NEOVLAŠTENI PRISTUP POVEZANIM VOZILIMA

SAŽETAK

Razvoj informacijsko-komunikacijskih tehnologija direktno doprinosi sve većem broju povezanih vozila na tržištu te njihovim učestalim korištenjem povećava se broj kaznenih djela koja se provode neovlaštenim pristupom u povezana vozila. Povezana vozila mogu sadržavati ključne podatke koji mogu pomoći u rješavanju određenih kaznenih djela poput krađe automobila, krađe identiteta, daljinskog nadzora pojedinca ili rješavanju prometnih nesreća u kojima su sudjelovala ili neposredno sudjelovala povezana vozila. Budući da razvoj informacijsko-komunikacijskih tehnologija direktno doprinosi razvoju povezanih vozila, analizom potencijalnih točaka za neovlašteni pristup povezanim vozilima smanjuje se broj neovlaštenih pristupa u povezana vozila primjenom raznih softverskih i hardverskih alata. U ovom radu analizirane su potencijalne točke za neovlašteni pristup povezanim vozilima te razvoj istih kako bi se smanjila mogućnost pristupa povezanim vozilima.Svrha je rada prikazati mogućnost i značajke, odnosno ograničenja i potencijalne točke upada u sustave povezanih vozila putem kojih osobe s neovlaštenim pristupom dolaze do materijalne ili druge koristi. Cilj istraživanja je prikazati koncept povezanih vozila, arhitekturu i komunikacijske tehnologije povezanih vozila te slabosti istih.Rad je izrađen analizom postojeće relevantne literature o temi, odnosno provedena je analiza sekundarne literature, znanstvenih članaka i knjiga uz korištenje interneta.

KLJUČNE RIJEČI:povezana vozila; neovlašteni pristup povezanim vozilima;točke za neovlašteni pristup povezanim vozilima

ANALYSIS OF THE POTENTIONAL POINTS OF UNAUTHORIZED ACCESS TO CONNECTED VEHICLES

SUMMARY

The development of information and communication technologies directly contributes to the increasing number of connected vehicles on market, and their frequent use increases the number of crimes committed through unauthorized access to connected vehicles. Connected vehicles can contain key data that can help solve certain crimes such as car theft, identity theft, remote monitoring of an individual or solve traffic accidents involving or directly involved connected vehicles. Since the development of information and communication technologies directly contributes to the development of connected vehicles, analyzing potential points for unauthorized access to connected vehicles reduces the number of unauthorized access to connected vehicles using varius software and hardware tools. In this paper are analyzed potential points for unauthorized accesss to connected vehicles and their development in order to reduce the possibiliy of access to connected vehicles.The purpose of the paper is to present the possibility and features, i.e. limitations and potential points of intrusion into the systems of connected vehicles through which persons with unauthorized access obtain material or other benefits. The aim of the research is to present the concept of connected vehicles, the architecture and communication technologies of connected vehicles and their weaknesses. The paper was created by analyzing existing relevant literature on the topic, that is, an analysis of secondary literature, scientific articles and books was carried out using the Internet.

KEYWORDS:connected vehicles; unauthorized accessto connected vehicles; points for unauthorized accesss to connected vehicles

Sadržaj

1. Uvod

Povezano vozilo je svako vozilo koje ima mogućnost komunikacije s uređajima u blizini putem bežičnih mreža. Razvoj informacijsko-komunikacijskih tehnologija doprinosi povećanju broja povezanih vozila te njihovog svakodnevnog korištenja. Najčešći slučajevi uporabe povezanih vozila koja se koriste u svakodnevnici su sustavi zabave koji se povezuju s mobilnim telefonom vozača do vozila povezanih s internetom koja ima dvosmjernu komunikaciju s drugim vozilima, mobilnim uređajima te prometnom infrastrukturom. Svaki oblik tehnologije ima svoje prednosti kao i mane. Korištenjem povezanih vozila povećava se izloženost distribuciji i gubitku podataka samog vozila kao i vlastitih podataka putem potencijalnih točaka za pristup povezanim vozilima. U ovom radu analizirat će se potencijalne točke pristupa povezanim vozilima te sigurnosni razvoj istih.

Svrha istraživanja je prikazati mogućnost i značajke, odnosno ograničenja i potencijalne točke povezanih vozila putem kojih osobe s neovlaštenim pristupom dolaze do materijalne ili druge koristi.

Cilj istraživanja diplomskog rada je prikazati koncept povezanih vozila, arhitekturu i komunikacijske tehnologije povezanih vozila te slabosti istih putem kojih osobe s neovlaštenim pristupom ulaze u sustav povezanih vozila.

Rad je teorijski te je izrađen analizom postojeće relevantne literature o temi, odnosno provedena je analiza sekundarne literature, znanstvenih članaka i knjiga uz korištenje interneta. Za vizualni prikaz prikupljenih podataka izrađene su tablice i grafovi koji su popraćeni tekstualnim tumačenjem.

Rad je podijeljen u sedam cjelina:

1. Uvod
2. Koncept povezanih vozila
3. Arhitektura i komunikacijske tehnologije povezanih vozila
4. Točke i mehanizmi neovlaštenog pristupa u povezana vozila
5. Motivacija i instrumenti za neovlaštene pristupe povezanim vozilima
6. Forenzička analiza povezanih vozila
7. Zaključak

Rad započinje uvodom u kojem je najavljena tema rada, kao i njegov cilj i svrha, a izložena je i struktura rada.

U drugom poglavlju rada prikazan je te detaljnije opisan koncept povezanih vozila te smjer razvoja koncepta povezanog vozila koje pomoću različitih senzora prikuplja podatke

unutar vozila, kao i iz okoline, te analizom podataka koji se prikupljaju u prometnom okruženju. Koncept povezanih vozila na različite načine komunicira unutar vozila, a postoje i drugi načini komunikacije s okolinom izvan povezanih vozila.

Treće poglavlje opisuje arhitekturu i komunikacijske tehnologije povezanih vozila. Detaljno su prikazane slabosti tehnologije povezanih vozila pomoću kojih osobe s neovlaštenim pristupom dolaze do podataka, te na koji način upravljaju povezanim vozilima.

Četvrto poglavlje najznačajniji je dio rada, a opisuje točke i mehanizme neovlaštenog pristupa u povezana vozila. Detaljnije su prikazane točke, mehanizmi te instrumenti kojima se osobe s neovlaštenim pristupom služe kako bi ušle u sustav i na taj način preuzele kontrolu povezanog vozila, ali i cjelokupnoga sustava kojim se povezano vozilo služi.

Motivacija i instrumenti za neovlaštene pristupe povezanim vozilima opisani su u petom poglavlju rada. Isti služe kako bi se proizvođači i korisnici povezanih vozila mogli privremeno i djelomično zaštititi od protupravnog korištenja podataka.

Šestim je poglavljem rada obuhvaćena forenzička analiza povezanih vozila. Budući da razvoj informacijsko-komunikacijskih tehnologija direktno doprinosi razvoju povezanih vozila, analizom potencijalnih točaka za neovlašteni pristup povezanim vozilima smanjuje se broj neovlaštenih pristupa u povezana vozila. Dok povezani automobili postaju mnogo sigurniji u prometu, mreže koje sadrže potencijalno sigurnosne komponente postaju nesigurnije. Za održavanje sigurnosnih značajki, sigurnosna i automobilska industrija trebale bi uspostaviti i održavati snažne sigurnosne sustave.

Zaključak je sažeta sinteza ukupnog rada.

2. Koncept povezanih vozila

Koncept povezanih vozila odnosi se na aplikacije, usluge i tehnologije koje povezuju vozilo s njegovim okruženjem. Povezano je vozilo ono vozilo u kojem postoji uređaj za povezivanje s drugim uređajima unutar istog vozila i/ili uređaja, te mrežom, aplikacijama i uslugama izvan vozila. Funkcije takvih povezivanja su, prije svega, sigurnost u prometu, parking asistencija, pomoć na cesti, dijagnostika na daljinu, autonomnost vozila, navigacijski sustav ili GPS (engl. *Global Positioning Systems*), napredni sustavi asistencije u vožnji ili ADAS (engl. *Advanced Driver Assistance Systems*), inteligentni sustavi prijevoza ili ITS (engl. *Intelligent Transportation Systems*) i dr. [1].

Razvoj ITS-a odgovor je na povećanje broja vozača i vozila, produljenje trajanja vožnji, odnosno porast različitih prometnih zahtjeva općenito. Prema istraživanju provedenom u Kanadi, 2012. godine,prosječno vrijeme putovanja na posao na posao i s posla povećalo se s 54 minute 1992. godine, na 65 minuta u 2010. godini [2]. U SAD-u, je trajanje putovanje na posao i s posla produljeno za šest minuta u odnosu na 44 minute u 1992. godini [3]. Osim čestih i brojnih gužvi na prometnicama, čest problem predstavlja i zatvaranje dijela cesta zbog građevinskih radova, a povećava se i smrtnost sudionika u prometu. Posljednji i najaktualniji prometni zahtjev odnosi se na smanjenje onečišćenja u skladu s ciljevima ekološke zaštite Zemlje i ljudi [4]. U nastavku će poglavlja biti opisana povijest razvoja povezanih vozila, trenutno stanje na tržištu povezanih vozila, kao i očekivani smjer budućeg razvoja povezanih vozila.

2.1. Povijest razvoja povezanih vozila

U ranoj fazi automobilske industrije, cilj razvoja vozila bio je postizanje što veće brzine vožnje. U kasnom 20. stoljeću zabrinutost potrošača o sigurnosti, udobnosti i učinkovitosti vožnje, postala je umjesto što veće brzine vozila, glavna motivacija i smjer razvoja automobilske industrije. Rezultat novih nastojanja automobilske industrije bio je ICV (engl. *Intelligent Connected Vehicle*), odnosno inteligentno povezano vozilo, koje je široko prepoznato i prihvaćeno kao obećavajuća tehnologija za sprječavanje prometnih nezgoda i poboljšanje učinkovitosti vožnje [5].

Unatoč suvremenoj računalnoj opremi i informacijsko – komunikacijskoj tehnologiji prisutnoj u sustavima povezanih vozila, ona nisu proizvod 21. stoljeća. Zapravo, prvo je povezano vozilo nastalo davne 1980. godine u trkaćem automobilu Formule 1. Povezane značajke Formule 1 bile su putno računalo kojeg je instalirao BMW. Tek desetljeće nakon toga, prvo je povezano vozilo prometovalo cestom. General Motors je zajedno s OnStar-om prvi izveo povezana vozila na cestu. Tri automobila modela *Cadillac* prva su koristile značajke povezanih vozila. Prva značajka, tada instalirana, bila je hitni poziv, a cilj je toga bio promocija sigurnosti i vožnji i dostupnosti pomoći nakon eventualne prometne nesreće [6].

Prvo je povezano vozilo prometovalo u vrijeme kada mobilne veze nisu bile pouzdane (kao što su danas), a General Motorsželio je stvoriti siguran i pouzdan proizvod te je glasovne pozive pozivnom centru, koji je kontaktirao hitne službe u slučaju nesreća, omogućio telematski sustav. Poziv hitnoj službi bio je upućivan u trenutku otvaranja zračnih jastuka, a s vremenom je sustavu dodana i mogućnost navigacijskoga sustava. 2001. godine uvedena je daljinska dijagnostika. 2003. godina obilježena je uvođenjem izvješća o stanju vozila i uređaja za pristup mreži. U ljeto 2014. godine Audi A3 bio je prvi proizvođač automobila koji je ponudio pristup 4G LTE (engl. *Long-Term Evolution*) Wi-Fi pristupnim točkama, a prvu masovnu implementaciju 4G LTE napravio je General Motors. Do 2015. godine OnStar je obradio milijardu zahtjeva kupaca te se povijest povezanih automobila nastavlja razvijati i postoje mnoge vrste povezanih automobila s naprednijim sigurnosnim značajkama prilagođenih željama kupaca[7]. Najvažnije prekretnice u razvoju povezanih vozila prikazuje tablica ispod.

Tablica 2.1. Ključni trenutci razvoja povezanih vozila [7]

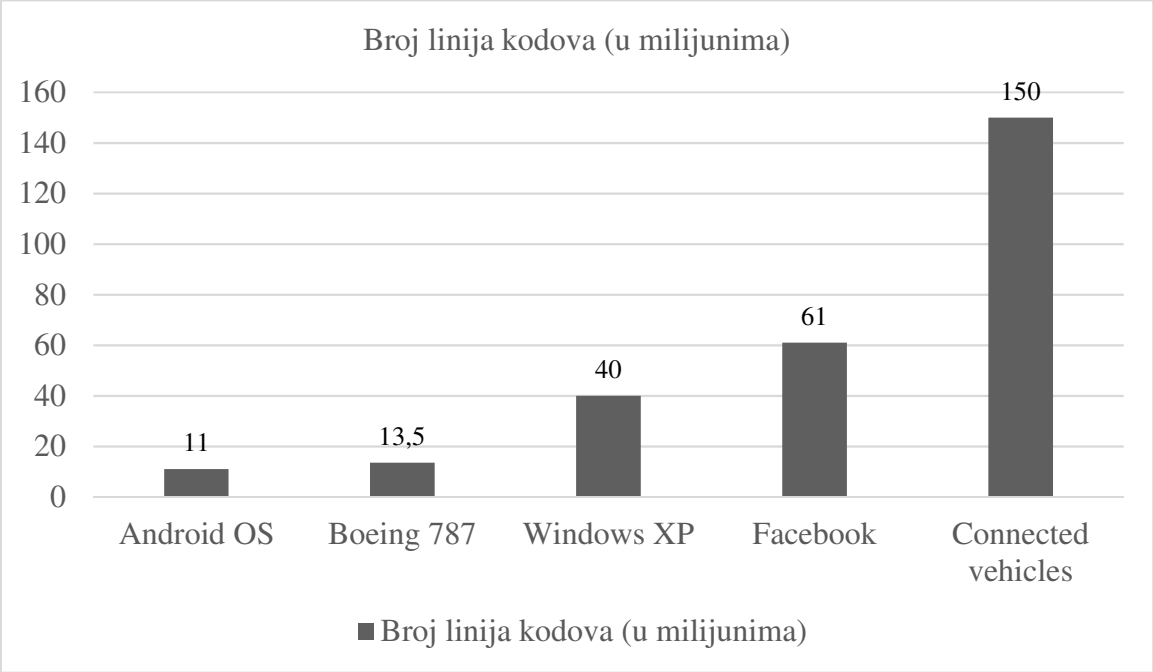
Godina	Područje noviteta	Opis mogućnosti
1996.	sigurnost	mogućnost poziva iz vozila doprinosi sigurnosti vozača i putnika
2001.	udaljena dijagnostika	telematski sustavi omogućuju udaljenu dijagnostiku vozila
2003.	uređaj za pristup digitalnoj mreži	izvješće o ispravnosti vozila i precizna navigacija vožnje
2016.	LTE	standardizacija telematike visoke brzine

Tablica iznad prikazuje razvoj povezanih vozila u dvadeset godina, a prvi značajan korak predstavlja naglasak na sigurnoj vožnji. Prva su povezana vozila imala mogućnost hitnog poziva u slučaju prometne nezgode, a to je funkcionalno od 1996. godine. Sljedeći napredak u sustavu povezanih vozila predstavlja udaljena dijagnostika iz 2001. godine, a samo dvije godine kasnije uvedeno je i izvješćivanje o stanju vozila (izvješće se šalje pristupanjem mreži). Od 2016. godine korištenje LTE standarda bežične komunikacije postaje standardno za sva povezana vozila.

2.2. Povezana vozila u sadašnjosti

Suvremena vozila nisu više tek mehanički sustavi jer su njihovi operativni programi i sustavi sklopljeni od više od sto milijuna linija kodova, što ih čini naprednijima od operativnoga sustava Boeinga 787. Operativni sustavi današnjih vozila počivaju na konceptu povezanosti, odnosno, vozila sliče računalima i imaju mogućnost sinkronizacije s mobilnim

telefonima, vozačima (i putnicima) mogu dati podatke o vremenskoj prognozi, ažurirane podatke o lokaciji (navigacijski sustav), odnosno razvojem informacijsko – komunikacijske tehnologije rastu i mogućnosti povezanih vozila, no to istovremeno označava i porast broja mogućnosti za hakere da neovlašteno pristupaju povezanim vozilima[8]. Usporedbu broja kodova u različitim suvremenim operativnim sustavima prikazuje graf ispod.



Graf 2.1. Milijuni linija kodova u različitim u suvremenim operativnim sustavima [8]

Kao što je vidljivo u grafu iznad, sustav povezanih vozila vrlo je složen, a prema broju linija koda daleko premašuje operativne sustava Androida, Boeinga 787, Windows XP-a i Facebooka.

ICV se definira kao vozilo sljedeće generacije koje je opremljeno naprednim senzorima i sustavima kontrole, a dizajnirano je za inteligentnu i kooperativnu vožnju koja jamči sigurnost vozača (i putnika), udobnost, energetsku učinkovitost te rasterećenje vozača pojednostavljenjem vožnje. ICV se prema SAE (engl. *Society of Automotive Engineers*) standardu dijeli u šest kategorija različitih razina inteligencije, a ta je podjela prikazana tablicom ispod. SAE standard podjele ICV- prihvatili su brojni proizvođači automobila diljem svijeta, poput Toyote, Nissana, Tesle i Audija[5].

Tablica 2.2. SAE standard različitih razina inteligencije ICV-a[5]

Razina inteligencije ICV-a	Karakteristike ICV-a	Primjer ICV-a
Razina 0	nema automatizacije, potreban je vozač za sve dinamičke zadatke vožnje	(nije ICV)
Razina 1	pomoć vozaču, kada se aktivira, moguća je ili uzdužna ili bočna kontrola vozila	2015 Infiniti Q50S; 2016 Lexus RX; 2016 Volvo XC90; BMW 750i xDrive; Mercedes- Benz E and S-Class
Razina 2	djelomična automatizacija, kada se aktivira, moguća je i uzdužna i bočna kontrola vozila	
Razina 3	uvjetna automatizacija, moguće je aktivirati izvršenje svih dinamičkih zadataka vožnje	Audi A8; Tesla Model S
Razina 4	visoka automatizacija, može izvesti sve dinamičke zadatke vožnje bez intervencije vozača, ipak zahtijeva intervenciju vozača u određenim načinima vožnje ili pojedinim geografskim područjima	Ford's Hybrid Fusion Research Vehicle; KIT and Ohio State University's AnnieWAY;Carnegie Mellon's Boss;Googles Research Vehicle; Baidu's Research Vehicle; Uber's Research Vehicle; Drive.ai Research Vehicle; Pony.ai Research Vehicle; MIT's Talos; Stanford's Junior; Virginia Tech's Odin; Apple's Research Vehicle(nabrojani ICV-i su još u fazi istraživanja i testiranja)
Razina 5	potpuna automatizacija, može izvršiti sve dinamične zadatke vožnje	

S obzirom na široki spektar tehnoloških mogućnosti i potencijala ICV-a, postoji i opsežna percepcija javnosti koja je zabrinuta za narušenje privatnosti, svoju sigurnost, visoke troškove, zaštitu osobnih podataka i sl.

Privatnost je glavna briga i javnog i privatnog sektora te bi briga o privatnosti trebala biti središnje razmatranje u odlukama proizvođača povezanih vozila o tome kako se informacije prikupljaju, arhiviraju i distribuiraju. Ipak, podaci prikupljeni putem povezanih vozila i drugih ITS aplikacija potencijalno bi mogli biti korisni za druge svrhe, primjerice, podatke mogu koristiti državni instituti za promet ili ministarstva prometa s namjerom analize obrazaca korištenja cesta, te tome primjereno planiranje održavanja i poboljšanja prometnica. Strah javnosti povezan za sigurnost odnosi se na opasnost od hakiranja sustava ICV-a, a kako će biti objašnjeno ovim radom, taj strah nije sasvim neopravdan, ali nije niti nerješiv problem za proizvođače povezanih vozila[9].ICV se još uvijek ne proizvodi masovno te prihvaćanje koncepta povezanih vozila, ostaje zadatak i izazov proizvođačima automobila za budućnost.

2.3. Očekivani razvoj povezanih vozila u budućnosti

Očekuje se da će inteligentna povezana vozila ili ICV značajno promijeniti živote ljudi u bliskoj budućnosti čineći prijevoz sigurnijim, čišćim, ekološki prihvatljivijim i udobnijim. Iako već postoji nekoliko prototipova ICV-a, a koncept autonomne vožnje je prisutan na različitim prometnicama svijeta, još uvijek postoji značajan jaz koji je potrebno prevladati prije mogućnosti masovne proizvodnje ICV-a [5].

Autonomno vozilo, odnosno vozilo koje se može samo voziti, predmet je interesa i fasciniranosti široke javnosti i to, prvenstveno, zbog svoje iznenađujuće inteligencije. Stoga, istraživački instituti, proizvođači automobila pa čak i IT tvrtke nastavljaju ulagati u tehnologiju povezanih vozila.

Međutim, transformacija tih inteligentnih sustava iz razvojne faze u fazu masovnu proizvodnju zahtijeva pomake u hardverskim i softverskim tehnologijama. Jaz koji trenutno postoji i usporava mogućnost masovne proizvodnje povezanih vozila odnosi se na razlike u gledištu proizvođača automobila, koji su usredotočeni na industrijski razvoj standardizirane opreme i stručnjaka različitih profila koji su usmjereni na razvoj inteligentnih algoritama, arhitekturu i komunikacijske tehnologije povezanih vozila. Nedostatak razumijevanja i suradnje rezultira jazom između dva svijeta. U svrhu ubrzanja razvoja autonomne vožnje, industrijske i akademske strane trebale bi raditi zajedno kako bi istinski integrirali razvoj automobilskog hardvera i softvera [5].

Tehnologija povezanih vozila utjecat će na modele dugoročnog korištenja zemljišta i planiranja izgradnja prometnica. Ceste i raskrižja sa semaforima obično se projektiraju na temelju ponašanja i osobina čovjeka. S obzirom da se ponašanje čovjeka znatno razlikuje od mogućnosti ICV-a koje, za razliku od ljudi, koristi sustave senzora kako bi se lociralo duž staze i komuniciralo s drugim vozilima i/ili infrastrukturom duž mreže, u budućnosti bi bilo moguće optimizirati geometrijski dizajn autocesta. Osim toga, masovno korištenje ICV-a značilo bi i poboljšanje kapaciteta prometnica jer, zbog naprednog sustava senzora, ICV-ovi mogu održavati manji međusobni razmak nego što je to slučaj kada vozilom upravlja čovjek. Isti sustavi senzora omogućili bi znatno smanjenje broja prometnih nesreća. Značajna prednost korištenja ICV-a u budućnosti je i održivi ekološki razvoj i smanjenje emisije štetnih plinova u atmosferu [9].

3. Arhitektura i komunikacijske tehnologije povezanih vozila

Suvremena su vozila revolucionarna zbog integracije distribuiranih ugrađenih sustava ili elektronički kontroliranih jedinica ili ECU (engl. *Electronic Control Units*), koje pružaju razne značajke i usluge poput navigacije, samoupravljanja, internetske veze, mogućnost glasovnih naredbi, dijagnostike i sl. Namjera je ovakvog tehnološkog razvoja vozila i zadovoljavanje potreba vozača za ugodnom i maksimalno sigurnom vožnjom [10].

U ovom će poglavlju detaljnije biti opisani komunikacijski protokoli CAN, LIN, AE, FlexRay i MOST, a zatim slijedi i njihova usporedba prema najvažnijim obilježjima sustava.

3.1. CAN

Jedan od najzahtjevnijih zadataka tijekom razvoja ICV-a je upravljanje komunikacijom između elektroničkih komponenti vozila čiji se broj, kao i složenost, neprestano povećavaju. Osim same prirode zadataka, zahtjevnim ga čine i visoki troškovi. S namjerom postizanja kontrole nad komunikacijom elektroničkih dijelova ICV-a razvijen je protokol mreže kontrolera ili CAN (engl. *Controller Area Network*). Objavio ga njemački Bosch, 1986. godine na SAE kongresu. U usporedbi s drugim mrežnim tehnologijama, CAN je bio (i ostao) mnogo uspješniji, i to prvenstveno zbog svoje isplativosti i fleksibilnosti[5].

CAN (engl. *Controller Area Network*) je jedan od najčešće korištenih komunikacijskih protokola koji implementira diferencijalni signal za prijenos poruka. Još od svoje pojave tijekom kasnih 1980-ih godina, uspješno se koristi za širok raspon funkcija, ali neprestano se razvoja i modernizira [10].

CAN prima i obrađuje informacije o vozilu koje se najčešće koriste za:

- upravljanje potrošnjom goriva,
- kontrolu točenja goriva,
- nadzor načina vožnje vozača (eko vožnja),
- nadzor sigurnosnih informacija (sigurnosni pojas, upaljena dnevna svjetla i sl.),
- kontrolu podsustava na vozilu (agregati, pumpe i dr.),
- kontrolu efektivnog radnog vremena, itd.

Jedna od istaknutijih značajki CAN-a uključuje*multi-master* serijski komunikacijski protokol s jednom sabirnicom koji emitirane poruke odašilje do svih povezanih čvorova na sabirnici, a može isporučiti poruke u rasponu od 50 kbit/s do 1 Mbit/s [10].

Standardni CAN podatkovni okvir sastoji se od nekoliko jedinstvenih polja s promjenjivom duljinom bitova, a ta su polja prikazana na slici ispod. Početak poruke je polje početak okvira ili SOF (engl. *Start of frame*), prepoznavanje poruke ili ID (engl. *Message*

Identifier). ID je 11-bitni identifikator koji određuje prioritet poruka koje su odaslane. Slijedi polje veličina podataka ili DLC (engl. *Data Length Code*), u kojem se informacije od 0 do 8 bajtova prenose u okviru poruke (engl. *Data*). Zatim, ciklička provjera redundantnosti ili CRC (engl. *Cyclic Redundancy Check*), nakon koje slijedi potvrda ili ACK (engl. *Acknowledgement*), a zatim i kraj okvira ili EOF (engl. *End of frame*). EOF čini 7 bitova logičkog (recesivnog) stanja, koje označava kraj okvira poruke i međuokvira ili IFS (engl. *Interframe Spacing*)[10].

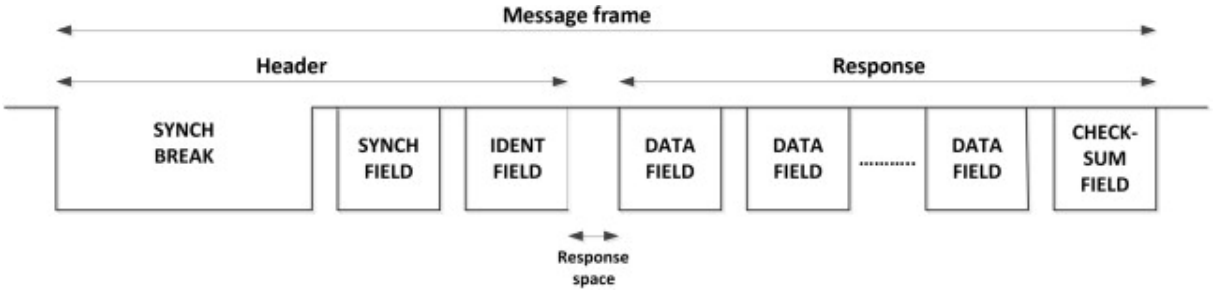
Slika 3.1. Ključni dijelovi CAN poruke [10]

3.2. LIN

Osim CAN-a, postoji i lokalna interkonekcijska mreža ili LIN (engl. *Local Interconnect Network*). To je široko primijenjena mreža koja, u usporedbi s CAN-om, omogućava više jeftinih i fleksibilnih žica jer je ista jednožična mreža. LIN se lako može implementirati na raznim vrstama kontrolera, čak i na 8-bitnim mikrokontrolerima, ali njegova maksimalna brzina prijenosa poruke može doseći tek 20 kb/s[5].

Iako se CAN pokazao kao vrlo pouzdankomunikacijski protokol, također je složen i skup. Ipak, ne zahtijevaju sve veze u okruženju motornih vozila punu sposobnost CAN-a te je, 1999. godine, razvijen LIN koji funkcionira uz CAN[11].

LIN protokol moguće je implementirati s bilo kojim mikrokontrolerom koji podržava UART modul. LIN protokol sastoji se od okvira, a svaki okvir ima dva dijela: zaglavlje i odgovor[12]. Strukturu LIN protokola prikazuje slika ispod.



Slika 3.2. LIN protokol[12]

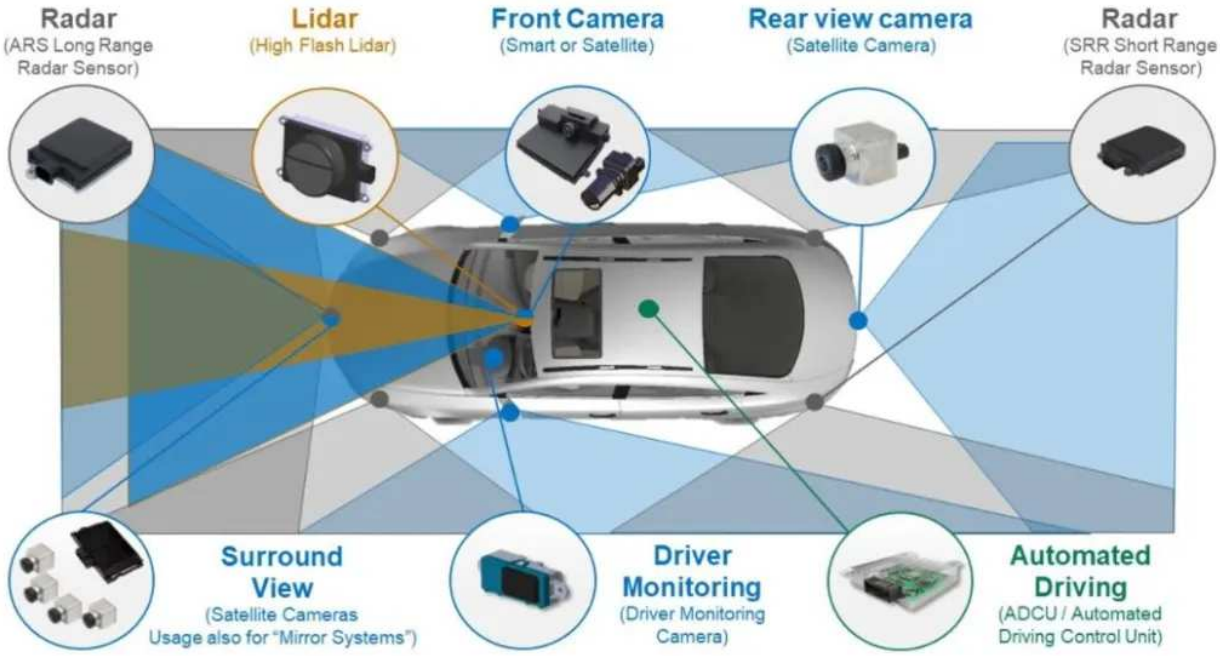
LIN podatkovni okvir sastoji se od zaglavlja i odgovora. Brzina prijenosa poruke u zaglavlju može biti od 1 do 20 Kbit/s. Zaglavlje čini polje proboj koje upozorava na dolaznu poruku, polje sinkronizacije i polje identifikacije u kojem se, na temelju poruke, odabire sljedeća radnja koja se poduzima. Odgovor je poruka od do osam bajtova[11].

Zanimljivo je da standard LIN uključuje i softverske elemente. LIN API (*Application Programmers Interface*) pruža skup standardnih C funkcijskih poziva, koji između sebe implementiraju sve LIN funkcije, što olakšava razvoj softvera i njegovo testiranje[11].

3.3. AE

Suvremeni napredak u komunikacijskim mrežama povezanih vozila uglavnom je koncentriranoko protokola AE (engl. *Automotive Ethernet*). AE je stara, ali nova komunikacijska tehnologija. Naime, ethernet je bila najčešća tehnologija za lokalne mreže u svijetu računala gotovo 45 godina, ali za potrebe automobilske industrije značajno je modificirana. Prva primjena AE u proizvodnji povezanih vozilabila je 2013. godine, za automobil BMW X5, a korišten je za povezivanje ugrađene kamere[5].

AE nudi najbolji omjer koristi i cijene za rukovanje brzim prijenosom podataka velike propusnosti. AE osigurava fleksibilnost i ekonomičnost, a sustav je otporan na okolinske smetnje poput topline, prljavštine i vlage. Integracija AE-a u vozila je jednostavna, a sustav se proteže kroz čitavo vozilo, pružajući širok raspon informacija o kritičnim sustavima i uređajima, šaljući podatke velikom brzinom. Strukturu AE-a u vozilu prikazuje slika ispod.

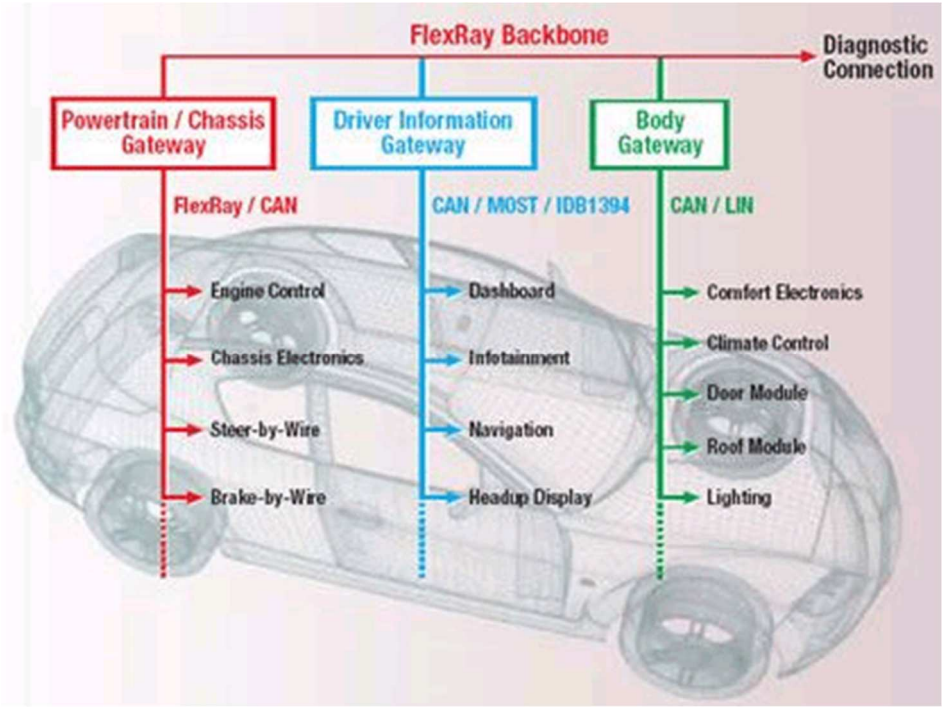


Slika 3.3. AE u vozilu [13]

AE u vozilu obuhvaća komunikacija između radara dugog i kratkog dometa, lidra, prednje i stražnje kamere, kamere za praćenje vožnje i snimanje okoline te sustava automatske vožnje.

3.4. FlexRay

FlexRay stvoren je da osigura ugrožene aplikacije povezanih vozila[5]. Protokol FlexRay dizajniran je da zadovolji zahtjeve današnje automobilske industrije, uključujući fleksibilnu podatkovnu komunikaciju, rad otporan na pogreške i prijenos većeg broja podataka nego što je to ranije bilo moguće. FlexRay omogućuje i asinkronizirani prijenos podataka, kao i prijenos podataka u stvarnom vremenu. FLexRayje dvokanalni sustav, a svaki kanal isporučuje maksimalnu brzinu prijenosa podataka od 10 Mbps. Protokol FlexRay pripada obitelji vremenski aktiviranih protokola koju karakterizirakontinuirana komunikacija svih povezanih čvorova preko redundantnih podatkovnih sabirnica naunaprijed definiranim intervalima[14]. FlexRay protokol u vozilu prikazuje slika ispod.

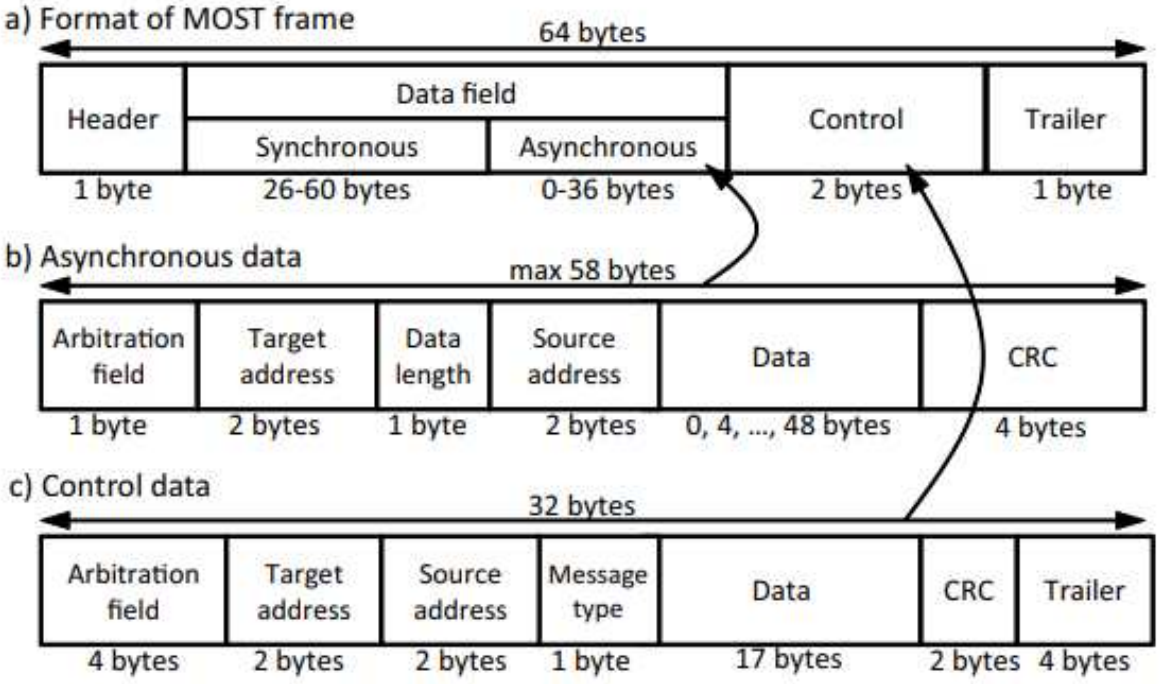


Slika 3.4. FlexRay u vozilu [15]

3.5. MOST

MOST (engl. *Media Oriented Serial Transport*) je dizajniran s namjerom postizanja veće brzine prijenosa podataka za podršku infotainmentu[5]. Protokol MOST mnogo je složeniji od drugih protokola (npr. CAN, LIN). Osnovna komunikacijska jedinica protokola kreirana je sa 16 okvira (slika ispod). Jedan okvir može biti dugačak do 64 bajta i može se koristiti za slanje podataka (sinkroniziranih, asinkroniziranih ili kontrolnih). Najčešći tip podataka je sinkronizirani, te oni zauzimaju najveći dio okvira. Asinkronizirani podaci koriste

se za podršku sinkroniziranih podataka. Kontrolni su podaci odgovorni za upravljanje komunikacijom između mrežnih priključaka[16]. MOST protokol i vrste podataka koje prenosi, prikazuje slika ispod.



Slika 3.5. Prijenos podataka MOST protokolom [16]

3.6. Usporedba komunikacijskih protokola povezanih vozila

AE je obećavajuća opcija mreže povezanih vozila zbog veće propusnosti, trenutni kapacitet propusnosti AE-a doseže 100 Mbps, a očekuje se i ažuriranje na 1 Gbps. U usporedbi s protokolima CAN i LIN, AE ima veću razinu sigurnosti. Poboljšana sigurnost temelji se slanju poruka IP-om, čime se otklanja opasnost da se jednim hakiranim ECU-om pristupi čitavoj ethernet mreži. Još je jedna prednost AE-a, u odnosu na druge protokole, što ga čini manje ECU-ova i kabela; s višom komunikacijom propusnosti, AE se može koristiti kao okosnica velike brzine pojednostaviti mrežu i smanjiti ECU i kabele. S obzirom da je AE stara tehnologija koja se mijenja i nastavlja koristiti, za nju postoje već izrađeni ISO standardi te sve više proizvođača automobila planira koristiti upravo AE protokol. Ipak, mnogi su primjeri suživota AE-a i drugih protokola, primjerice CAN protokola u jednom automobilu koji su se pokazali uspješnima [5].

Usporedba brzine slanja informacija, broja čvorova, duljine mreže, načina slanja poruka, financijskih troškova, dostupnosti između tehnologija povezanih vozila, koje su opisane u prethodnim poglavljima, prikazana je tablicom ispod.

Tablica 3.1. Usporedba komunikacijskih tehnologija povezanih vozila [5]

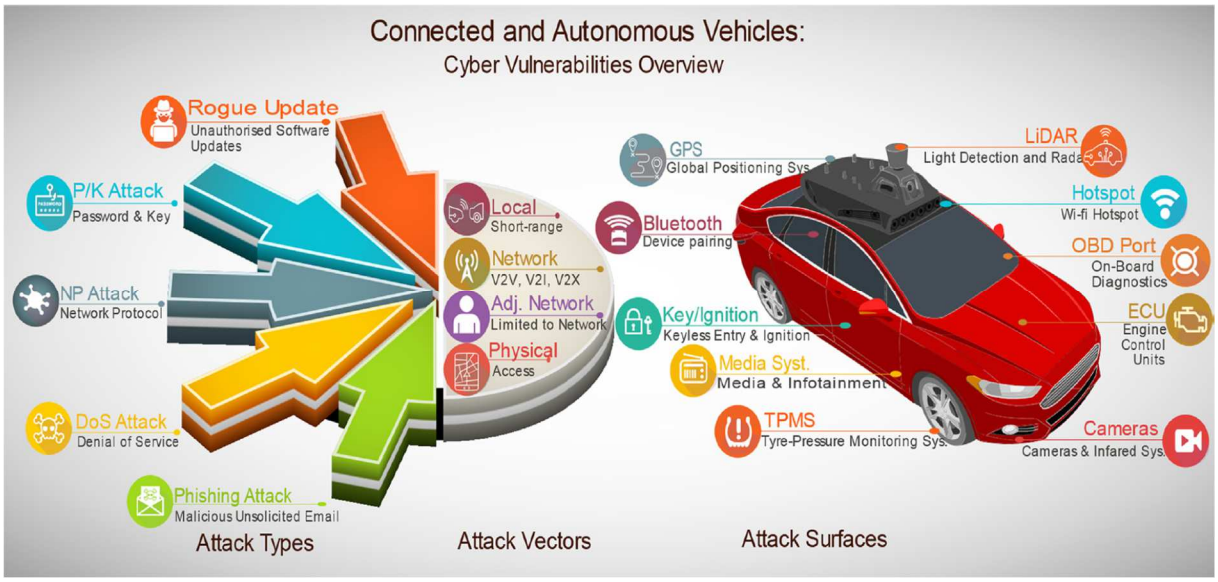
	CAN	LIN	AE	FlexRay	MOST
Propusnost (Mb/s)	1 ili 10	0,02	1000 (u razvoju)	20	150
Maksimalan broj čvorova	30	16	odgovara broju prekidača	22	64
Duljina mreže	40 m	40 m	15 m po vezi	24 m	1280 m
Slanje poruka	multi – master	master – slave	temelji se na IP-u	multi – master	ciklično, stream
Financijski trošak	nizak	izrazito nizak	visok	Nizak	visok
Sigurnost	pouzdana	nepouzdana	dokazana izvan automobilske industrije	Pouzdana	pouzdana
Dostupnost	mnogobrojna	mnogobrojna	u porastu	Nekoliko	jedna
Umreženje	UTP	jednožično	UTP	UTP	optički, UTP
Osnovne aplikacije	General bus	prekidači, vrata, sjedala	Infotainment, Backbone (u budućnosti)	Safety-critical, X-by-wire	Infotainment

4. Elementi i mehanizmi neovlaštenog upada u povezana vozila

Mnoštvo tehnologija za omogućavanje ugrađenih u povezana i autonomna vozila obećava prevenciju i ublažavanje nesreća, smanjenje emisija stakleničkih plinova i učinkovitije korištenje energije i prometne infrastrukture. U skladu s time, komunikacijska mreža u vozilu podržava sve veći broj elektroničkih upravljačkih jedinica (ECU). Primarni cilj vozila bez vozača je smanjenje smrtnih slučajeva na cestama koje uglavnom uzrokuju pogreške ljudskih vozača. Međutim, i u slučaju vozila bez vozača, ljudi predstavljaju najveću opasnost povezanim i autonomnim vozilima. Konkretno, riječ je o hakerskim napadima ili o *cyber* rizičnosti povezanih i autonomnih vozila. *Cyber* rizik definiran je kao rizik financijskog gubitka, poremećaja ili narušenog ugleda organizacije zbog neke vrste kvara u sustavu informacijske tehnologije. *Cyber* rizici su dinamične prirode zbog stalnih digitalnih inovacija, intenziviranja globalne povezanosti i sve veće sofisticiranosti hakera. *Cyber* rizik uvijek predstavlja potencijalnu štetu značajnih razmjera, no u slučajevima hakiranja povezanih vozila, potencijalna je opasnost posebno izražena jer su ugroženi ljudski životi vozača (i putnika).*Cyber* rizik neovlaštenog pristupa sustavu povezanih vozila nije tek paranoična ideja jer, konkretno, sustav suvremenog povezanog vozila čini i do 150 milijuna linija koda,koji usmjeravaju učinak rad do 70 ECU, a Windows operativni sustav čini 40 milijuna linija koda i, istovremeno, postoji 905 poznatih slabih točki sustava nabrojanih u NVD-u (engl. *National Vulnerability Database*). Te su ranjive točke bile aktivirane u široko rasprostranjenim *cyber* napadima u 2017. godini[17].

Povezivanjem vozila s vanjskim okruženjem povećava se broj mogućnosti za *cyber* napad te rizik od ranjivosti ubrzano raste. Različiti autori proučavaju mogućnosti hakerskih neovlaštenih upada te predlažu mjere za ublažavanje štete, kao i načine zaštite.Postojeća literatura bilježi nekoliko uspješnih kibernetičkih napada, primjerice Miller i Valasek su 2015. godine izveli daljinski hakerski napad na Jeep Cherokee uvođenjem zlonamjernih podataka u CAN protokol vozila. Pristupivši vozilu bili su u mogućnosti kontrolirati nekoliko elemenata vozila, uključujući sustav za kočenje.Autori ipak ističu da će do cyber napada povezanih vozila tek dolaziti, ali i da ranjivosti sustava povezanih vozila otkrivaju istraživači i hakeri *u bijelim šeširima*, odnosno da javnost ne treba osjećati strah od povezanih vozila [17].

Prikaz mogućih elemenata i mehanizma neovlaštenog pristupanja sustavima povezanih vozila, koji će biti opisani u nastavku poglavlja, prikazuje slika ispod.



Slika 4.1. Pregled različitih vrsta, modela i sredstava *cyber* napada na sustave povezanih vozila [17]

Tablica ispod prikazuje mogućnosti koje napadač stječe pristupanjem vozilu kroz određeni sustav vozila. Prema tim mogućnostima moguće je utvrditi i motive za napad.

Tablica 4.1 . Mogućnosti koje pruža neovlašten pristup povezanim vozilima [18]

Mogućnosti dobivene pristupanjem povezanom vozilu / motivi napada	**Elementi i mehanizmi neovlaštenog pristupanja povezanim vozilima**
Ometanje vozačkih operacija	LiDAR
	Radar
	GPS
	Kamere
	Uskraćivanje usluge mreže
Preuzimanje kontrole nad vozilom	LiDAR
	Radar
	GPS
Krađa informacija	CAN
	ECU
	LiDAR

Usporedbu ranjivosti primarnih potencijalnih točki neovlaštenog pristupa sustavu povezanih vozila prikazuje tablica ispod, a kao što je istaknuto, najrizičniji su Infotainment sustav, OBD i mobilne aplikacije.

Tablica 4.2. Primarne točke napada na povezana vozila [18]

Razina prijetnje za mogućnost hakiranja	Točka napada na povezana vozila
Niska razina	Zračni jastuci Motor
Srednja razina	Brave
Visoka razina	Mobilne aplikacije OBD Infotainment

Mogućnosti neovlaštenog upada u povezana vozila prikazuje slika ispod, a svaka će od tih mogućnosti biti pojašnjena u nastavku poglavlja.

Slika 4.2. Neovlašteni upad u sustav povezanog vozila [19]

Komunikacijski protokoli (engl. *Vehicle communication busses*) nabrojani i opisani u trećem poglavlju rada imaju različite točke ranjivosti o kojima je više riječi bilo u četvrtom poglavlju rada.

Rizik od neovlaštenoga upada u sustav povezanih vozila korištenjem mobilnih aplikacija neprestano raste te bi trebalo procjenjivati i potvrđivati sigurnost daljinskih aplikacija za vozila na mobitelima i sličnim uređajima, kao i aplikacije na upravljačkoj ploči vozila koje su u interakciji s njima [19].

Veća povezanost vozila omogućila je proizvođačima vozila da distribuiraju mobilne aplikacije za vozila, koje povezuju vozila s pametnim telefonima, povoljno omogućujući vlasnicima upravljanje značajkama poput daljinskog pokretanja, zaključavanja, otključavanja, praćenja lokacije i status vozila, i dr. Te aplikacije korisnicima omogućuju kontrolu pojedinih funkcija vozila na daljinu, s druge strane ulice ili svijeta. Iako korisnicima olakšavaju upravljanje vozilom, mobilne aplikacije imaju i nedostatak. Naime, te iste aplikacije koje korisnicima (i proizvođačima) pomažu u komunikaciji s vozilima također djeluju kao mogućnost ulaza za hakerski napad. Prema izvješću automobilske cyber sigurnosti iz 2022. godine, 7,3% od svih automobilskih *cyber*-napada između 2010. i 2021. godine izvršeno je korištenjem mobilnih aplikacija. Ipak, hakiranje sustava povezanih vozila uz pomoć mobilnih aplikacija nije novost. Još 2016. godine azijski je proizvođač povezanih vozila onemogućio mobilnu aplikaciju otkrivši da je hakerima lako iskoristiti aplikaciju za neovlašteni pristup vozilu. Osim toga, 2019. godine zabilježeno je nekoliko slučajeva kada su vlasnici vozila koji su koristili mobilne aplikacije za daljinsko lociranje, otključavanje i pokretanje svojih vozila, imali pristup tuđim računima i informacijama o drugim vozilima. Osim toga, u kolovozu 2020. vlasnik vozila sjevernoameričke proizvodnje otvorio je mobilnu aplikaciju svog vozila, a aplikacija mu je prikazala pet automobila parkiranih u Europi. Mogao je vidjeti sve detalje tih automobila i kontrolirati ih na daljinu [20].

Usluge povezanih vozila koje su posebno osjetljive, odnosno rizične za hakerski napad, uključuju lokator vozila, daljinsko otključavanje i pokretanje te praćenje stanja voznog parka [19].

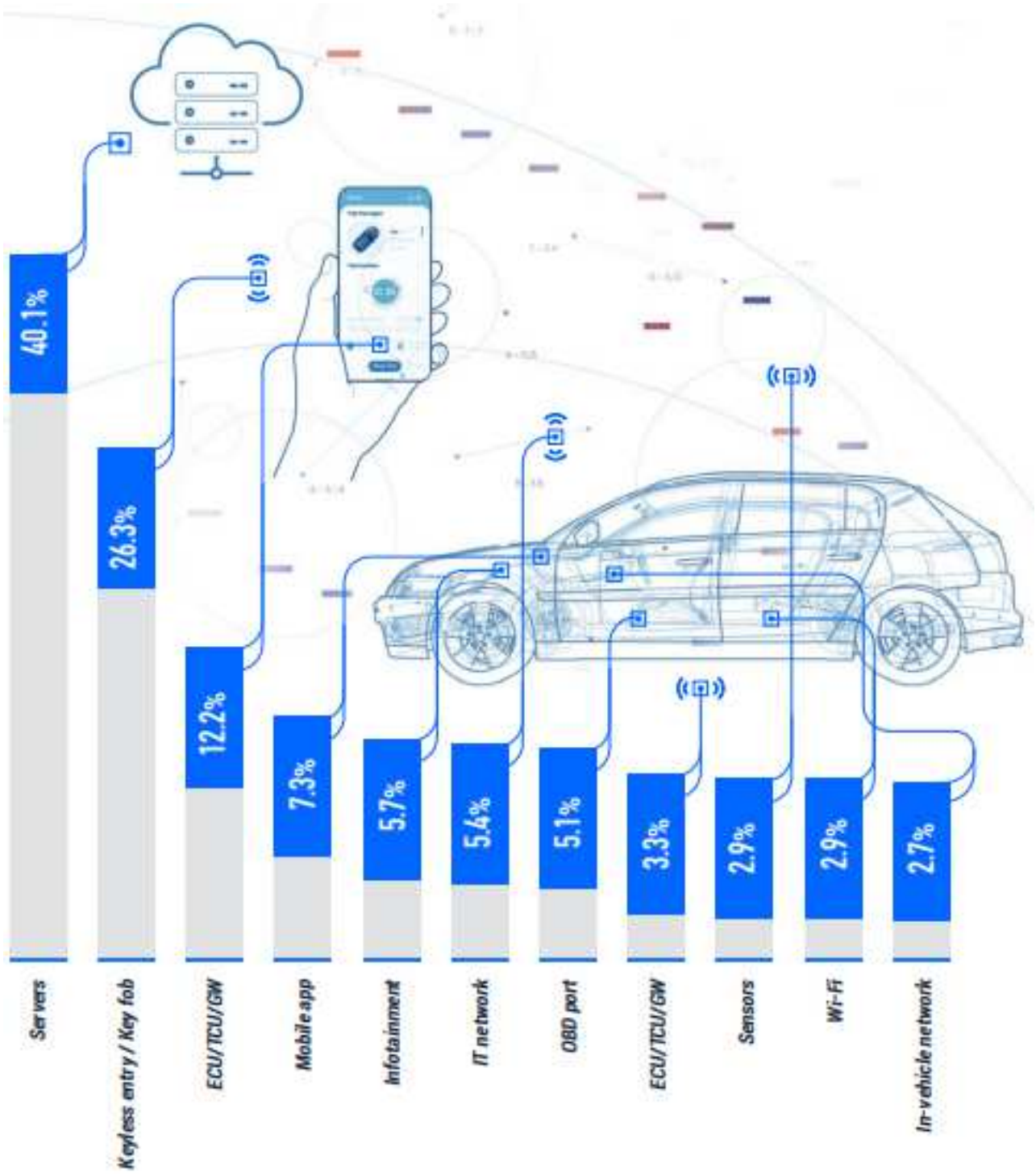
Govoreći o integriranoj sigurnosti vozila, dobavljači i proizvođači automobila trebali bi razmotriti način blokiranja napada na fizičke sigurnosne sustave vozila kao što su imobilizator, alarmni sustavi i sustavi za otključavanje. Osim toga, nužno je razmotriti i ublažiti napade na vozila putem radijske frekvencije [19].

GPS ili navigacijski sustav, USB, CD/DVD i druga fizička sučelja lako su dostupna i nude hakerima potencijalno uporište za ulazak u sustav s izravnim pristupom ugrađenim komponentama. Jednako su potencijalno opasne i tehnologije bežične komunikacije, poput Wi-fi-ja, Bluetootha, mobilnog interneta i sl. [19].

Napredni povezani sustavi vozila kao što su radar, kamere, sustavi za pomoć pri vožnji i parkiranju te sustavi za sprječavanje sudara nude napadačima vezu koja premošćuje jaz od *cyber* napada do fizičkog. Pod kontrolom hakera, ti se sustavi mogu koristiti za ugrožavanje temeljne sigurnosti vozila [19].

Slika ispod prikazuje učestalost hakerskih napada s obzirom na metodu ulaska. Najbrojniji, čak 40,1 % svih *cyber* napada, čine napadi na poslužitelje vozila. Poslužitelji pohranjuju informacije koje vozilo prikuplja, a često su informacije meta napada, a ne samo

vozilo. Poslužitelji imaju zadatak primati i slati podatke, a to ih čini ranjivima, jer u tom procesu mogu primiti zlonamjerni softver [20].



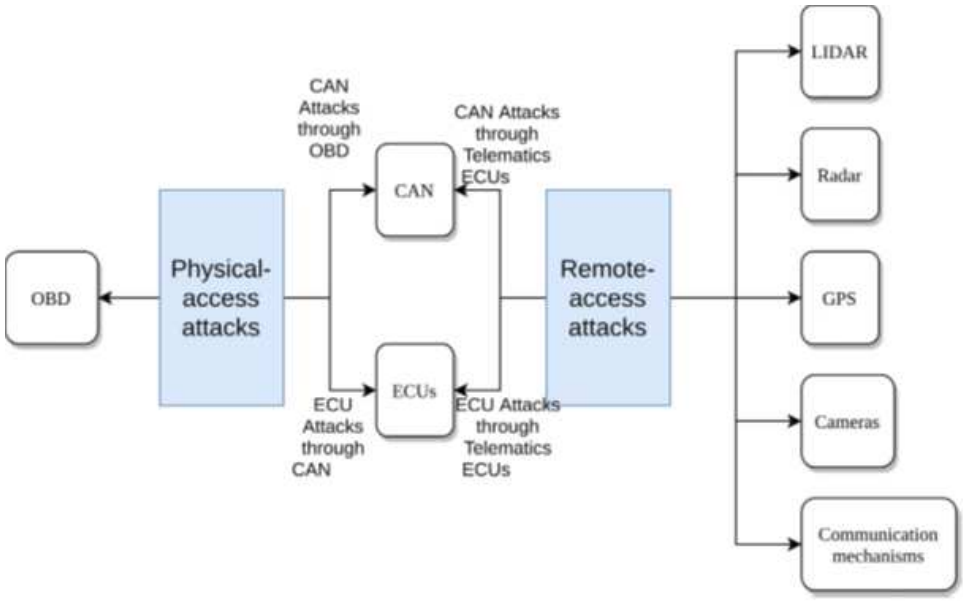
Slika 4.3. Najčešći napadi na povezana vozila [20]

Sažet pregled postojećih potencijalnih točki neovlaštenog pristupanja povezanim vozilima, uz postojeće obrambene strategije i izazove otpora prijetnjama napadača, prikazuje tablica ispod.

Tablica 4.3. Pregled postojećih hakerskih napada i strategija obrane sustava povezanih vozila [21]

Elementi i mehanizmi neovlaštenog pristupa povezanim vozilima	Strategija neovlaštenog pristupanja povezanim vozilima	Strategija obrane od napada na povezana vozila	Izazovi
GPS	Napadač emitira netočan, ali realističan GPS signal za prevaru GPS prijamnika vozila.	Obrambene strategije uključuju praćenje snage GPS signala, praćenje satelitskih signala i provjeru vremenskih intervala iz signala.	Učinkovitost obrane i protumjera nije sasvim poznata.
	Napadač emitira snažan signal kojim preopterećuje GPS prijamnik vozila te on ne može otkrivati prave signale.	Računanje vjerojatnosti napada korištenjem informacija iz GPS prijamnika.	Obrana je izvediva samo do određene razine snage ometajućih signala.
LiDAR	Napadači stvaraju krivotvorene signale koji predstavljaju predmet u blizini vozila.	Obrambene strategije uključuju korištenje više senzora koji se preklapaju, odašiljanje impulsa u nasumičnim smjerovima te nasumičan odabir oblika valova impulsa.	Obrambene strategije tek treba testirati.
	Napadači odašilju svjetlo jednake valne duljine, ali veće intenzivnosti, što ometa senzore LiDAR-a za primanje legitimnih svjetlosnih signala.	Obrambene strategije uključuju često mijenjanje valne duljine te korištenje više senzora.	Obrambene strategije tek treba testirati.
OBD	Uz fizički pristup OBD priključku, napadači mogu presretati prijenos podataka, prikupljati informacije, i unositi zlonamjerne podatke i softvere.	Korištenje *hardware-in-the-loop* opreme.	Vrlo je teško razlikovati legitimne od zlonamjernih OBD priključaka.
	Pristupanjem preko OBD-a, napadači mogu primati i slati poruke iz CAN-a.	Osiguravanje autentičnosti i pouzdanosti CAN poruka.	Nedostatak računalnih kapaciteta.
ECU	Kompromitiranje ECU-ova kroz CAN.	Osiguravanje OBD priključka i CAN poruka.	Teškoće u osiguravanju OBD priključka i CAN poruka.

S obzirom na vrstu pristupa, na daljinu je moguće pristupiti LiDAR sustavu, radarima, GPS sustavu, kamerama te komunikacijskim sustavima vozilima. Neovlašten pristup ECU-ovima, također je moguće izvesti na daljinu, a kroz ECU-ove vozila, napadač može pristupiti i CAN-u. Fizički je pristup nužan jedino za korištenje OBD priključka s namjerom neovlaštenog ulaza u vozilo, a podjelu napada prema vrsti pristupa prikazuje slika ispod.

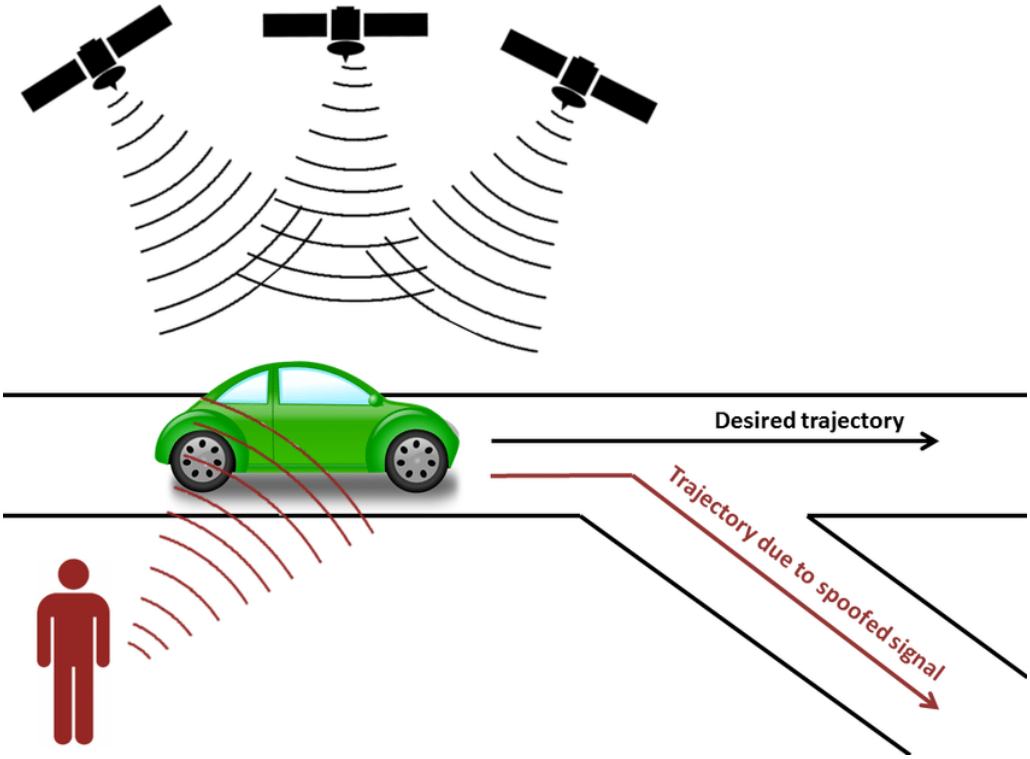


Slika 4.4. Mogući ulazi u povezana vozila napadom na daljinu i fizičkim pristupom vozilu [21]

4.1. GPS

GPS je satelitski navigacijski sustav koji financira i posjeduje vlada SAD-a, a njime upravljaju i održavaju Zračne snage SAD-a. Konkretno, to je globalni navigacijski sustav koji radi na temelju satelita u Zemljinoj orbiti koji odašilju visokofrekventne radijske signale. Radio signale mogu osjetiti mnogi uređaji kao što su pametni telefoni i GPS prijemnici u povezanim (i autonomnim) vozilima. Kada GPS prijamnici nekog uređaja prime signale s tri ili više satelita, mogu izračunati lokaciju na kojoj se taj uređaj nalazi. Budući da je pronalaženje rute između dvije lokacije neophodno za autonomnu vožnju, GPS signali su ključni za povezana (i autonomna) vozila. GPS prijamnici mogu raditi bez ikakvog komunikacijskog kanala kao što su bežične mreže, ali podaci iz bežičnih mreža često mogu povećati točnost GPS prijamnika [21].

Suvremeni sustavi povezanih vozila oslanjaju se na GPS za pružanje točnih ipravovremenih informacija, međutim dokazano je da je GPS rizičan i podložan *cyber* napadima te postoji nekoliko primjera već izvršenih hakerskih napada.



Slika 4.5. Prikaz neovlaštenog ulaza u vozilo kroz GPS sustav vozila [22]

Model napada - lažiranje GPS signala je napad u kojem napadač emitira netočne, ali realistične GPS signale kako bi zavarao GPS prijemnike na povezanim vozilima. Ta se metoda naziva i GPS spoofing, a proces zavaravanja GPS prijamnika vozila odvija se postupno - postupnim povećavanjem snage krivotvorenih signala. Ova je metoda potencijalno uspješna jer je GPS uređaj konfiguriran za korištenje signala s najjačim magnitudama. Stoga, kada je krivotvoreni signal jači od legitimnog satelitskog signala, GPS uređaji obrađuju krivotvoreni signal[21].

Primjerice, još 2013. godine studenti sa Sveučilišta u Teksasu pokazali su kako mogu generirati krivotvorene GPS signale koji bi postupno nadjačali autentične GPS signale. Napadač, dakle, u ovoj (spoofing) metodi treba samo nadjačati izvorni GPS signal. Hardver uključen u napad iz 2013. Godine razvili su Humphreys i suradnici, a prema njihovom vlastitom priznanju, jedino je njihov izum sposoban za precizno generiranje krivotvorenih GPS signala [22]. Napadači su utvrdili su da napadač mora moći izračunati udaljenost od sebe do cilja napada s pogreškom od najviše 22,5 metara te je uspješan napad GPS prijamnika na povezanom vozilu koje se kreće još uvijek neproveden, a napadom iz 2013. godine pogođeni su sustavi jahte[21].

Zeng i sur. (2018) sastavili su mali uređaj od popularnih komponenti ukupne cijene od 223 američka dolara i upotrijebili ga za pokretanje lažne navigacije od skretanja do skretanja kako bi žrtve doveli do krivog odredišta, a da ne budu primijećeni. Autori su demonstrirali napade na stvarne automobile s 40 sudionika i bili su u mogućnosti voditi 38 sudionika do

unaprijed određenih lokacija autora (95% uspješnosti). Zeng i sur. raspravljali su o jednom od ograničenja njihove studije, a to je da metoda napada nije učinkovita ako je vozač upoznat s područjem. Međutim, to možda nije slučaj za povezana vozila i stoga bi model napada Zenga i drugih predstavljao značajnu prijetnju povezanim vozilima. Osim toga, Regulus Cyber LTD. testirao je lažiranje GPS-a na vozilu Tesla 3 i uspješno natjerao GPS automobila da prikazuje lažne pozicije na karti pa je svaki pokušaj pronalaženja rute do odredišta rezultirao lošom navigacijom.Ukupni trošak opreme za izvođenje ovog napada bio je 550 američkih dolara, a u izvješću je također navedeno da je tu tehnologiju lako nabaviti, odnosno da je široko dostupna [21].

4.2. Bluetooth

Bluetooth, kao alat neovlaštenog pristupa vozilu, vrlo je moćan alat jer je moguće uvjeriti Bluetooth uređaj da smo mu blizu, čak i sa značajne udaljenosti, ali prava je opasnost u tome što je Bluetooth ranjiv čak i kada su poduzete obrambene mjere poput enkripcije i ograničenja latencije. Posebno je zabrinjavajuće to što je hardver za uspješan Bluetooth napad vrlo povoljan i široko dostupan [23].

Ta greška u Bluetooth prijemnicima potencijalno bi mogla utjecati na velik broj ljudi, a ne samo vozača. Primjerice, na organizacije koje zaključavaju vrata zgrada, na pojedince koji žele zaključati automobile, telefone, prijenosna računala ili druge osobne uređaje, itd. Stoga se proizvođačima preporuča da ograniče rizike napada na vozila onemogućavanjem funkcije blizinske tipke kada je korisnikov telefon nepomičan određeno vrijeme. Također predlažu dvofaktorski model autentifikacije. Vozačima se predlaženda omoguće značajku "*PIN to Drive*", kao i da isključe Bluetooth kada ga ne koriste[23].

Checkoway i sur. (2011) također su istraživali mogućnosti napada na povezana vozila ulaskom kroz Bluetooth. Obrnutim su inženjeringom uspjeli pristupiti ECU-ovom operativnom sustavu i upravljati određenim Bluetooth funkcijama [24].

4.3. Keyless Entry

Keyless entry označava ulazak u vozilo bez ključa, a postoje četiri vrste takvog bežičnog upadanja u vozila:

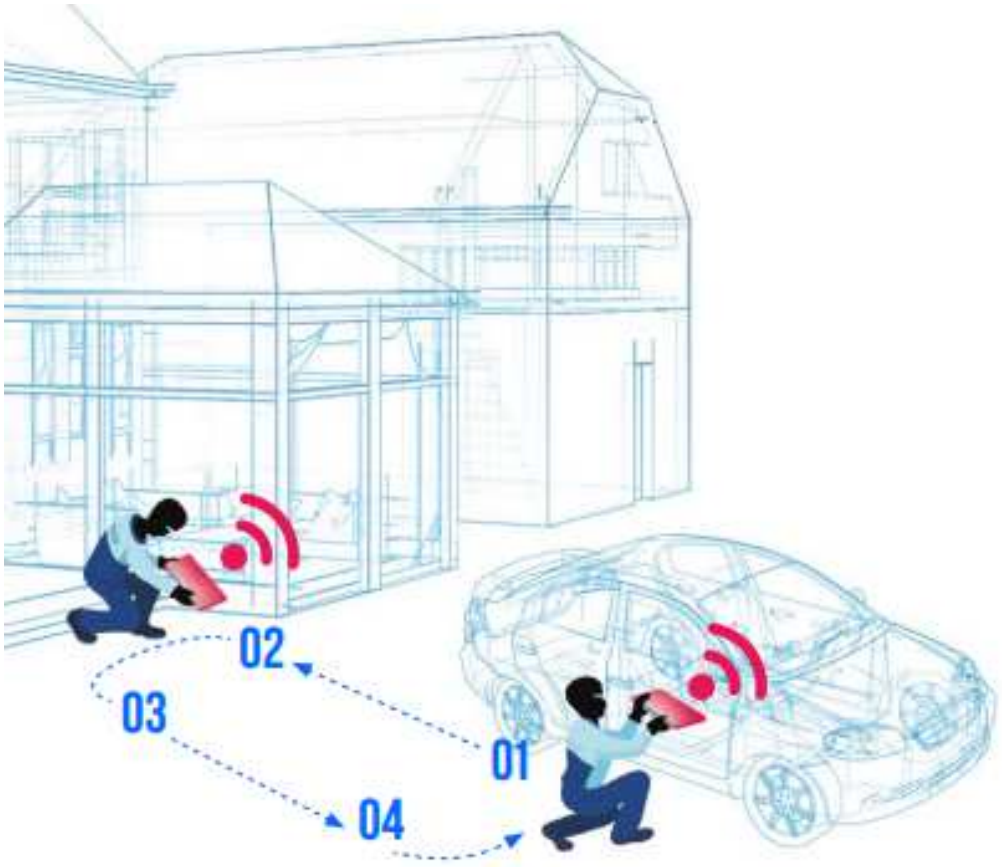
- relay ulazak,
- OBD ključ,
- ometanje signala ključa i
- spoofing[25].

Relay ulazak u vozilo označava proces preuzimanja radio signala s privjeska za ključeve, potencijalno unutar kuće vlasnika vozila.Preuzeti se signal zatim prosljeđuje na uređaj u blizini automobila, čime se sustav vozila *zavarava* da vlasnik ulazi u automobil bez ključa [25]. Neovlašteni pristup vozilu korištenjem OBD ključa detaljno je objašnjen nekoliko poglavlja niže.

Ometanje signala ključa tehnika je koja uključuje blokiranje signala koji dolazi iz ključa vozila. Vlasnik vozila je ključem zaključao vozilo, no zbog napadača koji su omeli taj signal iz ključa, vozilo nije zaključano. Otključanom vozilu svatko može pristupiti te je krađa vozila značajno olakšana.

Spoofing označava proces u kojem napadač krade kriptografski ključ vozila. Taj proces može trajati svega par sekundi. Ovu su tehniku uspješno demonstrirali hakeri u bijelim šeširima na Teslinom modelu vozila S [25].

Korake mogućeg načina krađe vozila bez ključa prikazuje slika ispod. Prvi je korak da jedan napadač stoji blizu vozilu šaljući signal drugome napadaču koji je u blizini kuće vlasnika vozila. Drugi napadač ima a uređaj za hakiranje te, u drugom koraku krađe, usmjerava taj uređaj u kuću, na mjesto gdje bi se ključ vozila mogao nalaziti. U sljedećem koraku, on prvome napadaču prenosi informacije od toga ključa. Posljednji korak je da prvi napadač, koji je u blizini vozila, dobivenim informacijama otključa vozilo i uđe u njega [20].



Slika 4.6. *Keyless entry* proces krađe vozila [20]

4.4. Infotainment

Infotainment sustavi u vozilu ili IVI (engl. *In-vehicle infotainment*) jedna su od najranjivijih jedinica povezanih vozila. Izloženi su različitim softverima, aplikacijama, mobilnim i Bluetooth uređajima. Ranjivost postoji jer vozači često povezuju svoje uređaje, poput pametnog telefona, s vozilom, čime dopuštaju pristup svojim privatnim informacijama, kontaktima, porukama, fotografijama i sl. Rizik za vozilo je u tome što je infotainment vjerojatno spojen na CAN vozila, te IVI može biti ulazna točka za napad na ECU-ove vozila [20].

Checkoway i sur. (2011) raspravljali su o napadu na infotainment sustav korištenjem CD playera kao ulazne točke. Identificirane su dvije ranjivosti, a prva se odnosi na mogućnost latentnog ažuriranja u *media playeru* kojiće automatski prepoznati ISO 9660 formatCD s posebno imenovanom datotekom koju će, kriptiranjem poruke, predstaviti korisniku. Ako korisnik ne pritisne odgovarajuću tipku, umetnuta će datoteka uništiti sustav i sve informacije koje sadrži. Osim toga, s obzirom da *media player* može analiziratisložene datoteka, istraživači su izvršili obrnuti inženjering značajnekoličine firmware-a te sumogli modificirati WMA audio datoteku tako da se reprodukcijom CD-a, koji sadrži zlonamjernu datoteku, odabrani paketi podataka CAN busa šalju u mrežu [24].

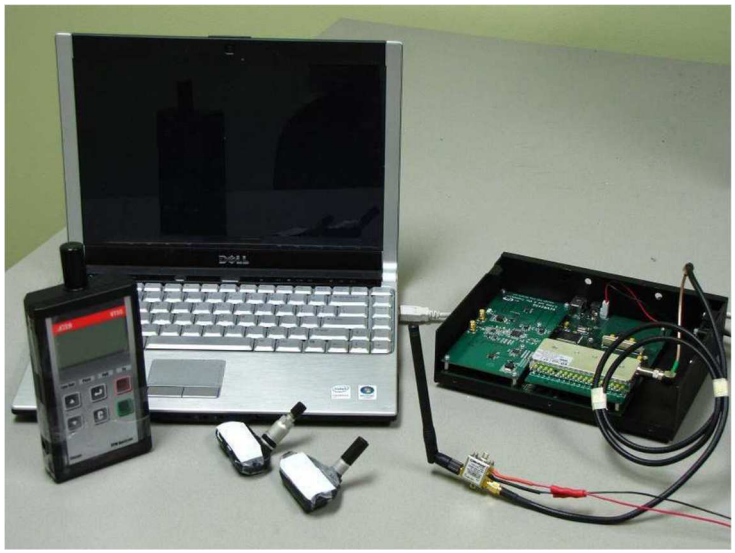
Primjerice, u svibnju 2021. istraživači su otkrili brojne ranjivosti u infotainmentu europskog proizvođača povezanih vozila koje bi se, potencijalno, mogle iskoristiti za hakiranje internih sustava vozila[20].

4.5. TPMS

TPMS (engl. *Tire Pressure Monitoring System*) je sustav upozorenja za mjerenje tlaka zraka u gumama pomoću senzora tlaka ili za praćenje pojedinačnih brzina vrtnje kotača koji upozorava vozača kada su gume premalo napuhane, odnosno obavještava vozača kada je tlak u gumama vozila nizak. Sigurnosni problem povezan s TPMS-om je taj da se vozilo može pratiti korištenjem postojećih senzora duž prometnica[26].

Jedan od ECU-a, sustav za nadzor tlaka u gumama (TPMS), može biti napadnut ugrožavanjem mjerenja (tlak/temperatura) koje emitira TPMS senzor. Napad se može proširiti preko na druge ECU-ove jer ECU-ovi dijele protokole. TPMS ECU analizira informacije primljene od TPMS senzora i otkrivaju status tlaka u gumama, a te informacije zatim prikazuje vozaču. Informacije koje emitiraju TPMS senzori mogu biti meta hakerskih napada. Napadač može snimiti svoju poruku i zatim je poslati vozaču, a naročitu opasnost predstavlja to što napadom na TPMS ECU napadač može pristupiti drugim ECU-ovima vozila jer su spojene na CAN protokol [27].

Ranjivost TPMS-a, istraživali su Roufa i sur.[28], a njihovo je istraživanje pokazalo da postoji razlog za zabrinutost vozača.Naime, Roufa i suradnici su, u suradnji s USRP-om (engl. *Universalom Software Radio Peripheral*), obrnutim inženjeringom pristupili vozilu na daljinu. Taj je upad u sustav vozila bio moguć jer se TPMS komunikacije temelje na standardnim modulacijskim shemama i jednostavnim protokolima, a ne na kriptografskim mehanizmima.Zaključili su da je prisluškivanje sigurno moguće na udaljenosti od otprilike 40 metara od vozila u pokretu. Rezultati njihova istraživanja pokazali su da se TPMS poruke mogu potpuno primiti na udaljenosti do 10 m od auto s jeftinom antenom i do 40m s osnovnim niskošumnim pojačalom. To znači da napadač može preslušati ili lažirati prijenose s ceste ili eventualno iz obližnjeg vozila.Slika ispod prikazuje alat kojim su Roufa i sur. neovlašteno pristupali TPMS sustavu povezanog vozila.



Slika 4.7. Oprema za neovlašteni pristup povezanom vozilu kroz TPMS [28]

TPMS nije najkritičnija komponenta povezanog vozila, ali i *samo* prisluškivanje predstavlja značajnu prijetnju privatnosti vozača i putnika. Osim toga, spoofing napadi koji ukazuju na problem s tlakom zraka u gumama mogu uzrokovati zaustavljanje vozača na nepreglednim mjestima ili samotnim lokacijama, što napadačima može olakšati krađu vozila nespremnog vozača ili nešto gore [24].

4.6. Lidar

LiDAR (*Light Detection and Ranging*) označava aktivni sustav daljinskog očitavanja svjetlosnim valovima. Taj sustavkoristi laserski puls za mjerenje udaljenosti do objekata mjerenjem vremena leta laserskih impulsa koji se odašilju do površine objekta i odbijaju od njega. Namjena ovog sustava je izbjegavanje sudara, prilagodljivi tempomat, i prepoznavanje objekata u blizini vozila [29].

Tri su vrste mogućeg neovlaštenog pristupa sustavu povezanih vozila preko Lidar sustava, a to su:

- napad neprijateljskog vozila,
- radovi na vozilu i
- korištenje infrastrukture uz rub prometnice [29].

Tipični napadi na sustave usmjereni su na prevaru algoritama koji uzimaju podatke iz LiDAR-a. Međutim, ova vrsta napada je vrlo teška zbog preciznog vremena u kojem laser pulsira na ciljnom LiDAR-u točnosti do nanosekunde[29].

Strategija napada funkcionira ispaljivanjem laserskog pištolja u LiDAR senzor autonomnog vozila kako bi se dodale lažne podatkovne točke. Utvrđeno je da autonomno vozilo može prepoznati napad ako su ti lažni podaci u velikoj suprotnosti s onim što njegova kamera vidi. Ali 3D LIDAR podatkovne točke, koje su pažljivo postavljene laserom unutar određenog područja 2D vidnog polja kamere, mogu prevariti sustav. Ovo ranjivo područje proteže se ispred objektiva kamere u obliku – 3D piramide bez vrha (engl. *frustum*). Ako napadački laser postavi nekoliko podatkovnih točaka ispred ili iza drugog automobila u blizini, percepcija tog automobila može se pomaknuti i za nekoliko metara. Taj takozvani *frustum* napad može zavarati tempomat vozila da misli da vozilo usporava ili ubrzava. U trenutku kada sustav otkrije da postoji problem, ne postoji način neagresivnog izbjegavanja sudara [30].

Postojeće obrambene strategije protiv lažiranja LiDAR signala obuhvaćaju:

- korištenje višestrukih senzora koji imaju preklapajuće prikaze,
- smanjenje kuta primanja signala,
- odašiljanje impulsa u nasumičnim smjerovima te
- nasumično raspoređivanje valnih oblika impulsa[21].

Ipak, autori su također istaknuli da ove obrambene strategije nisu uvijek sasvim odgovarajuće. Naime, korištenje više senzora izrazito je skupo. Smanjenje kuta prijema signala također je vrlo skupo jer zahtijeva više LiDAR uređaja za pokrivanje čitavog prostora oko vozila. Odašiljanje impulsa u nasumičnim smjerovima izvedivo je i jeftino, ali nije izravno učinkovito jer LiDAR uređaj mora poslati mnogo neiskorištenih impulsa. Stoga je nasumično raspoređivanje valnih oblika impulsanajprivlačnije rješenje zahvaljujući niskoj cijeni i visokoj učinkovitosti [21].

4.7. Wi-fi

U travnju 2021. hakeri s bijelim šeširom uspjeli su hakirati ECU koji kontrolira vrata vozila sjevernoameričkog proizvođača vozila korištenjem drona koji je nosio wi-fi adapter. Pristupivši vozilima, hakeri su ugrozili parkirane automobile, a kontrolirali su i infotainmenet sustave vozila, odnosno, mogli su upravljati mrežnim vezama i naredbama za vozila. Hakeri

su primijetili da bi bilo moguće upravljati i otključavanjem vrata i prtljažnika, promjenom položaja sjedala i načinom ubrzanja, ali ne i manipulirati kretanjem vozila. Dok se Wi-Fi veza može koristiti za veću produktivnost, pa čak i zabavu putnika tijekom prijevoza, otvara mogućnost hakerskog napada, kojamože omogućiti pristup CAN-u [20].

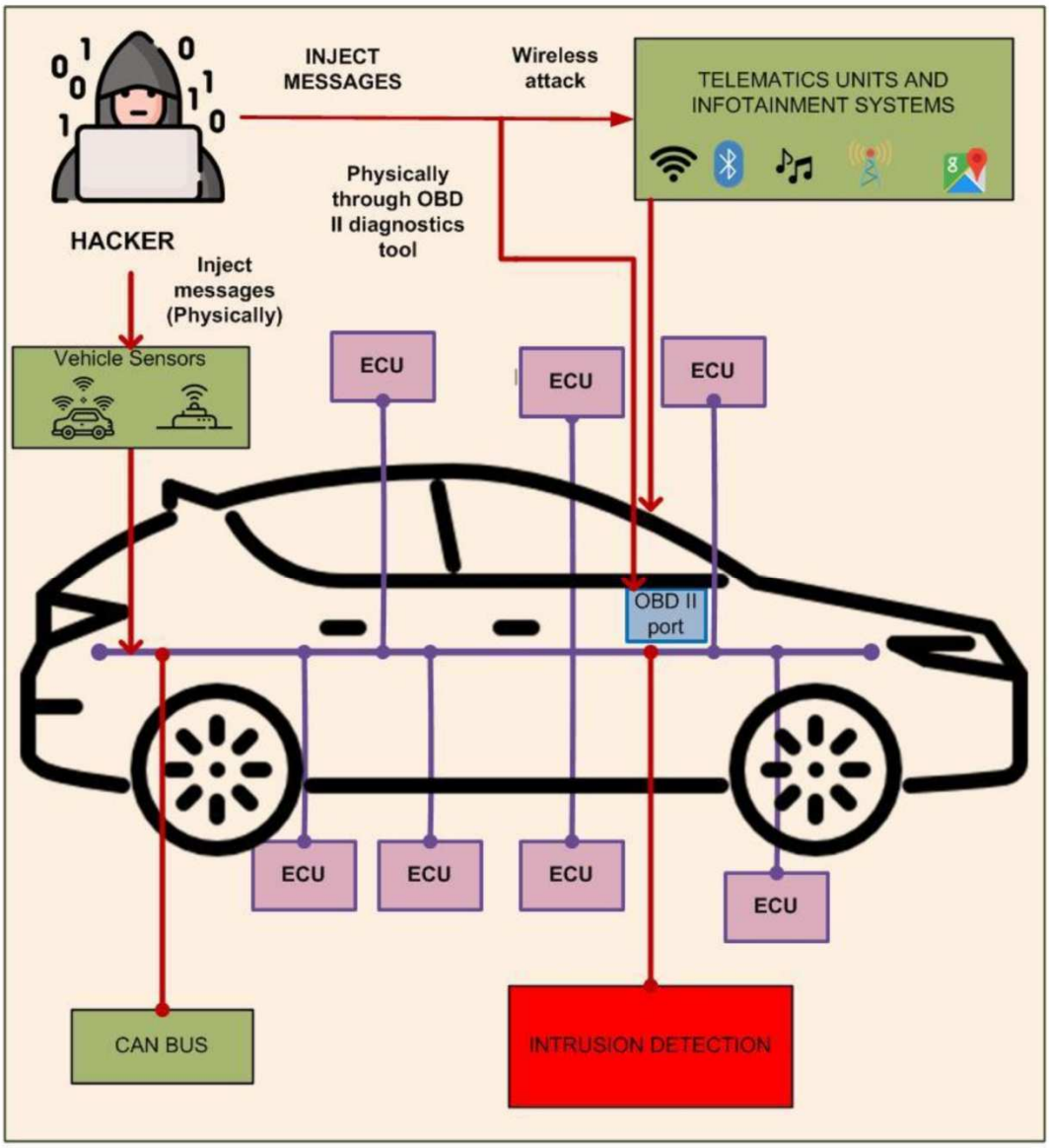
U lipnju 2021. istraživači bliskoistočnesigurnosne tvrtke otkrili su novu skup kritičnih ranjivosti u Wi-Fi modulu. Ove su ranjivosti dovoljne da haker s crnim šeširom potencijalno preotme bežičnu komunikaciju uređaja, a to rezultira manipulacijom automobilskih podataka. Ipak, nakon tih saznanja, u novim su verzijama firmvera ti problemi otklonjeni[20].

Charlie Miller i Chris Valasek su 2015. godine preuzeli kontrolu nad vozilom Jeep Cherokee i to bežično, ušavši kroz wi-fi sustav. Ipak, da bi ovaj napad bio izvediv, vlasnik vozila trebao bi uključiti wi-fi [24].

Vozač tog vozila, Andy Greenberg, opisao je kako je izgledao napad i što su Miller i Valasek kontrolirali na daljinu. Najprije su upalili hlađenje na najjače, promijenili radio stanicu i pojačali zvuk. Zatim su uključili brisače i aktivirali tekućinu za pranje stakla koja je zamaglila pogled vozaču. Vozač je pokušavao vratiti kontrolu nad vozilom, a tada su mu hakeri pokazali svoju sliku na zaslonu automobila. Za ovaj je napad vozač znao, te je i bio u dogovoru s hakerima za testiranje njihovih mogućnosti, a čitav je ovaj događaj imao za namjeru ukazati na ranjivost vozila Jeep Cherokee. Osim opisanoga, vozač se našao i na autocesti, a hakeri su tada isključili ubrzanje vozila.

4.8. OBD

Implementacija OBD (engl. *On-Board Diagnostics*) sustava je obveznau vozilima koja se prodaju u Sjedinjenim Državama od 1996. godine - u vozilima s benzinskim pogonom u Europskoj uniji od2001. godine, a u vozilima s dizelskim motorom u Europskoj uniji od 2004. godine. OBD je prvenstveno namijenjen kako bi vozilo moglo prijaviti svaki problem u svojoj infrastrukturi i poslatidijagnostičke podatke prikupljene vlastitim senzorima pružatelju usluga izvan vozila. OBD ključevi se koriste za dijagnostiku vozila, a njima je moguće pristupiti CAN protokolu vozila. OBD priključci smatraju se ulaznim točkama za napad na ECU koji su spojeni na CAN. Automobilski virus moguće je ubaciti u ECU preko OBD-a i pokrenuti određene poruke na CAN-u. Problem za sigurnost predstavlja to što OBD ključeve može kupiti bilo tko, i to vrlo jeftino. Osim toga, dodatnu opasnost predstavlja to što za neovlašteni pristup vozilu više nije potrebno fizički spojiti OBD ključ, jer moderna vozila vrše samodijagnostiku korištenjem *wi-fi* veze, a OBD ključevi su u obliku aplikacije [26]. Slikom ispod prikazani su koraci *cyber* napada povezanog vozila korištenjem OBD ključa.



Slika 4.8. Cyber napad izvediv korištenjem OBD ključa [31]

Strategija obrane povezanih vozila uključuje:

- provjera autentičnosti OBD uređaja,
- provjera integriteta OBD uređaja,
- provjera privatnost OBD uređaja te
- proces autentifikacije OBD uređaja[21].

Provjera autentičnosti OBD uređaja znači provjeru izvora, odnosno je li proizvođač uređaja pouzdana. Provjera integriteta OBD uređaja znači istraživanje učinkovitosti uređaja i provjeravanje je li uređaj bio oštećen ili ugrožen, nakon što je proizveden. Provjera privatnosti OBD uređaja označava da su sve informacije dobivene s OBD priključka razumljive su samo osobi kojoj je uređaj namijenjen.

4.9. ECU

Moderni automobil zapravo je računalno kontroliran stroj s desecima ECU-ova koji se, u okruženju povezanog vozila, povezuju na internetsku mrežu.Upravo je to povezivanje izvor ranjivosti sustava, naime, u vrijeme kada se vozilo nije povezivalo na mrežu, bila je dobra ideja da se kritični sustavi automobila izgrade na CAN-u, dok je sadašnjost povezanih vozila zbog toga ugrožena. CAN-u, pa i svim ECU-ovima moguće je (i lako) pristupiti korištenjem OBD ključa [32], a to prikazuje slika iznad.

U lipnju 2021. godine istraživači su potvrdili izvedivost ranjivosti *proof-of-concept* napada na dva vozila. Istraživači su pokrenuli disrupciju napada na dva vozila, iskorištavajući činjenicu da ECU-ovi često implementiraju značajku*time-out* koja sprječava CAN da zadrži dominantnost. Uspjeli su isključiti jedan od ECU pogonskog sklopa vozila i ECU servo upravljača drugog vozila. Pretpostavka istraživača je da su mnogi moderni automobili, vjerojatno, ranjivi na ove vrste napada, ali napadač bi morao najprije ugroziti mrežu vozila prije pokretanja ove vrste napada. Oni vjeruju da, kada napadač ima kontrolu nad određenom komponentom u vozilu, može, neotkriveno, utjecati na rad druge komponente[20].

Checkoway i sur. uspjeli su postići daljinsko izvršavanje koda na ECU-ovima vozila putem Bluetootha i bežične veze velikog dometa. To su postigli ekstrakcijom firmware-a ECU-a i korištenjem disasemblea (računalnoga programa koji dekompilira strojni kod u asemblerski jezik). Nakon procjene firmvera ECU-a koji je odgovoran za Bluetooth veze, autori su pretpostavili da, ako napadači mogu upariti svoje pametne telefone s Bluetooth ECU-om, onda mogu kompromitirati ECU slanjem zlonamjernog koda putempametnih telefona. Primjerice, obrnutim inženjeringom operativnog sustava ECU-a koji je odgovoran za rukovanje Bluetooth vezama, Checkoway i sur. pronašli su više od dvadeset nesigurnih poziva *strcpyju*, od kojih bi im jedan omogućio kopiranje podataka i, na taj način, izvršavanje bilo kojeg koda na ECU-ove [21].

Obrambena strategija ECU-ova povezanih vozila obuhvaća:

- robustan kod na firmware-u ECU-a kako bi se izbjeglo ubacivanje koda,
- ograničavanje pristupa povezivanju s telematskim ECU-ima,
- robusni protokoli ažuriranja firmvera [21].

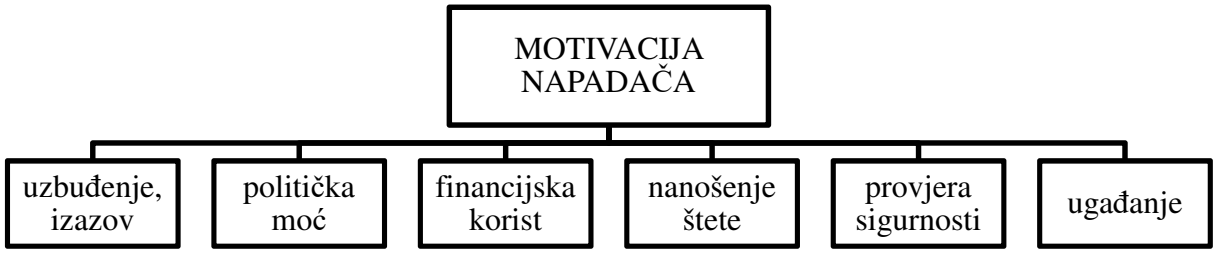
Robustan kod na firmwareu služi za izbjegavanje ubacivanje zlonamjernih kodova, a isti cilj ima i ograničavanje pristupa udaljenim ECU-ovima, odnosno preporuča se dozvoljavanje pristupa samo provjerenim i sigurnim izvorima. Robusni protokoli ažuriranja firmvera za ECU osiguravaju cjelovitost i autentičnost ažuriranja firmvera[21].

5. Motivacija za neovlaštene upade u povezana vozila

Razvojem povezanih vozila razvija se i raspon sigurnosnih rizika za neovlašteni upad u sustave vozila. Osim fizičkog pristupa vozilu, mnogi su načini i hakerskih napada na daljinu. Istraživači, ali i anonimni hakeri uspjeli su hakirati sustav povezanih vozila kompromitirajući TPMS, i to uz jeftinu i široko dostupnu opremu. Veći (i opasniji) problem predstavlja kada se vozila spajaju na ugrađeni Wi-fi sustav jer to sposobnim napadačima omogućava da kompromitiraju više vozila. Kompromitirana vozilo se također može koristiti za napad na druga vozila. Primjeri šteta koje *malware* (zlonamjerni softver) može nanijeti sustavu povezanih vozila:

- zaključavanje radija u automobilu kako ga korisnici ne bi mogli uključiti,
- proizvoljno uključivanje zvuka u automobilu i podešavanje glasnoće,
- brisanje ili mijenjanje datoteka na vozilu i na uređajima korisnika koji su povezani na vozilo,
- trošenje memorijskog prostora i CPU ciklusa,
- krađa privatnih podataka,
- onemogućavanje sigurnosnih funkcija vozila i
- slanje lažnih podataka drugim vozilima [33].

Različite količine rizika i potencijalne štetne posljedice neovlaštenih pristupa povezanim vozilima različito motiviraju napadače, a Hoppe i sur. su motivaciju napadača podijelili na kategorije prikazane slikom ispod.



Slika 5.1. Motivacija napadača da napadne povezano vozilo [34]

Uz vojnu snagu i ekonomsku moć, kibernetičke sposobnosti postale su još jedna skrivena sila kojom zemlje mogu utjecati na događaje u svijetu. Mnoge nacionalne države danas ciljaju svoje protivnike cyber kampanjama koje se kreću od špijunaže i infiltracije do različitih ransomware napada. Uobičajene mete uključuju vladine agencije, operatere infrastrukture, pružatelje zdravstvenih usluga, škole i tvrtke. S obzirom da se ekosustav povezanih automobila nastavlja širiti, nacionalne države mogle bi ciljati vozila i cestovnu infrastrukturu kako bi dobile velike podatke o cestovnoj mreži zemlje, uključujući pojedinosti o lokacijama kamera i semafora, kao i kretanja u prometu. Podaci koji otkrivaju identitet

povezani sa svakim vlasnikom vozila također se mogu iskoristiti za pokretanje ciljane infiltracije i phishing kampanja protiv pojedinaca visokog profila.U najgorem scenariju oružanog sukoba, neprijateljske države mogle bi čak pokušati poremetiti prometnu infrastrukturu kako bi izazvale prometni kaos i nesreće[35].

Haktivisti su samoorganizirani hakeri koji ciljaju na određene vlade ili organizacije kako bi podigli svijest javnosti o određenim političkim ili društvenim uzrocima. Za one koji žele ciljati na proizvođača automobila ili regionalnu vladu, pokretanje napada na povezane vozne parkove ili prometnu infrastrukturu može biti brz i učinkovit način da se njihov glas čuje. U veljači 2022. godine nepoznati haker napao je dobavljača Toyotinih ključnih komponenti prisilivši proizvođača da prekine rad na 24 sata. U budućnosti bi sličan napad mogao biti usmjeren izravno na vozni park, a moguća šteta bi bila daleko veća [35].

Skupine kriminalaca financijski su motivirani napadači koji postavljaju ransomware na ciljane mreže za šifriranje sustava i krađu osjetljivih podataka. Žrtve su tada prisiljene platiti otkupninu ako žele da im se sustav dekriptira ili da spriječe objavljivanje ili prodaju ukradenih podataka. U ovom scenariju, napadači su na dobitku u svakom slučaju te je njihova motivacija vrlo opasna za vozače i proizvođače povezanih vozila. Osim ostvarivanja financijske koristi, napadači mogu vozila koristiti i kao alat za počinjenje zločina. Na primjer mogli bi dobiti daljinski nadzor nad parkiranim vozilom i preusmjeriti ga na udaljeno područje pod svojom kontrolom kako bi ukrali osobne stvari vlasnika. Također,potencijalno bi mogli kontrolirati ta vozila za ilegalnu trgovinu i skrivanje zabranjene robe. Ipak, ovaj je scenarij još uvijek, zbog svoje iznimne složenosti, izvediv samo u teoriji[35].

Govoreći o kriminalcima koji neovlašteno pristupaju povezanim vozilima, s namjerom ostvarivanja financijske koristi, Raichard Hayton detaljnije opisuje koje su to skupine napadača:

- teroristi,
- ucjenjivači,
- vlasnici vozila,
- prethodni vlasnici vozila,
- automehaničari,
- proizvođači automobila,
- vlade te
- trgovci, graditelji cesta, urbanisti, ekološki nastrojeni ekstremisti, putnici[36].

Dobra vijest je da su tehničke poteškoće ulaska u sustav povezanog automobila mnogo veće nego u poslovnom sustavu. Čak i ako se ransomware uspješno implementira, otkupnina koju napadač može iskoristiti od pojedinačnog vlasnika vozila vrlo je ograničena. Stoga su napadi ransomwareom na privatna vozila vrlo malo vjerojatni u doglednoj budućnosti. Alternativno, napadači bi mogli pokušati zaraziti poslužitelje OEM-a kako bi onemogućili OTA usluge i ukrali osjetljive podatke vlasnika vozila, prisiljavajući OEM-a da izvrši plaćanje.

Dok haktivisti ciljaju na organizacije, terorističke skupine ciljaju na građane. Terorističke skupine u budućnosti bi također mogle pokrenuti razorne napade na povezane automobile i cestovnu infrastrukturu kako bi izazvale strah u javnosti. U ekstremnom slučaju, mogli bi čak pokušati preuzeti kontrolu nad autonomnim vozilom na daljinu i manipulirati vozilom kako bi izazvali sudar.

Nekoliko je mogućih razloga zašto bi teroristi pristupali povezanim vozilima. Za početak, kibernetički napad može biti daleko jednostavnije izvesti nego što bi to bilo postavljanje bombe pod vozilo jer se, između ostaloga, može učiniti na sigurnoj udaljenosti u za napadača. Osim toga, povezanost vozila povećava opseg napada, a time raste i motivacija napadača. Posljednji u nizu razloga je i preciznost napada. Aktivistička skupina koja digne u zrak čak i jedan automobil izgubit će puno simpatija te se cyber sigurnost može promatrati kao blaža opcija. Zaustavljanje grada stvaranjem velikog područja zagušenja ne košta (izravno) ljudske živote [36].

Vlasnici automobila visoko su motivirani da nezakonito podešavaju postavke, odnosno hakiraju sustav vozila. Konkretno, vlasnik vozila može željeti omogućiti neku(izvorno nepredviđenu) opcijsku mogućnost sustava, onemogućiti limitator brzine, i sl. Uvođenje takvih promjena često uključuje onemogućavanje sigurnosnih mogućnosti što istovremeno čini druge napade, često zlonamjerne prirode, daleko lakšima [36].

Prethodni vlasnici često mijenjaju podatke o vozilu s namjerom lakše prodaje, ali osim prevare kupca, motivacija za hakiranje može biti i puno veća te je moguće da prodavač vozila ostavi uključene postavke koje omogućuju jednostavno praćenje vozila i nakon što je prodano kupcu [36].

Automehaničari hakiranjem i promjenom podataka o vozilu mogu više naplatiti „potrebne“ popravke, ali, ono što je opasnije, mogu ugraditi zlonamjerne softvere u vozilo s namjerom budućeg napada na vozilo. Također, pristup različitom broju marki i modela vozila za kriminalno nastrojenog mehaničara predstavlja kvalitetan trening i upoznavanje „plijena“ [36].

Proizvođači automobilaovise o povjerenju kupaca te teže maksimalnoj sigurnosti svojih automobila, no te se težnje nimalo ne odnose na vozila koje proizvode konkurenti. Pokaže li se vozilo koje proizvodi konkurencija nepouzdano, prodaja takvih vozila će zasigurno pasti što znači da će kupci, u većem broju, kupovati vozila trećeg proizvođača [36].

Motivacija vlade za pristupanje vozilima uglavnom se temelji na špijunaži, otkrivanju tajni neprijatelja i osiguravanje političke moći i prevlasti [36].

S obzirom na različite vrste motivacije za napade povezanih vozila, za automobilsku industriju iznimno je važno analizirati i predvidjeti tko bi mogli biti potencijalni počinitelji i zašto bi željeli pokrenuti napad kako bi bila ispred potencijalnih kriminalaca. Ta se predviđanja zatim mogu koristiti za usmjeravanje procesa TARA (engl. Threat Assessment and Remediation Analysis) ili procjena prijetnji i analiza sanacije, nakon čega slijedi testiranje napada i uvježbavanje obrane[35].

Podaci o načinima neovlaštenih upada u sustave povezanih vozila pokazuju da je čak 84,5% napada izvedeno na daljinu, dok je samo 15,5% napada uključivalo fizički pristup vozilima. Primjer napada kratkog dometa dogodio se u Ujedinjenom Kraljevstvu u srpnju 2021. kada je vozilo europske proizvodnje hakirano i ukradeno izvan doma njegova vlasnika iskorištavanjem i zlouporabom sustava daljinskog ulaska bez ključa. Napadači su koristili uređaj za relay napad uperivši ga u kuću vlasnika kako bi aktivirao kontakt i aktivirao vozilo, a zatim su se odvezli ukradenim automobilom. Iako napade na daljinu uglavnom izvode hakeri u bijelim šeširima, stručnjaci predviđaju da će se ta djelatnost proširiti i na drugu vrstu hakera[20].

Slika 5.2. Odnos hakerskih napada na povezana vozila dalekog i kratkog dometa [20]

U nastavku poglavlja detaljnije će biti objašnjeni mogući razlozi neovlaštenih upada u sustave povezanih vozila te koje vrste napadača, a zatim i kojim se instrumentima koriste za napad sustava povezanih vozila.

Razumijevanje onoga što bi motiviralo napadače da šire zlonamjerni softver na vozila ključno je za razumijevanje rizika i utjecaj napada zlonamjernog softvera. Nekoliko vjerojatnih motiva za neovlaštene upade u povezana vozila su:

- zabava i publicitet,
- kršenje privatnosti vozača,
- otkupnina,
- krađa vozila,
- sabotaža,
- ozljeđivanje ljudi,
- ometanje transporta [33].

Mnogi sigurnosni napadači hakiraju računala samo radi zabave ili da bi dokazali svoje vještine, odnosno ukazali na slabosti računalne zaštite drugih, te se predviđa se da će mnogi hakeri rastuću populaciju povezanih automobila smatrati jednako zanimljivim *hobijem*. Hakiranje automobila moglo bi stvoriti veći publicitet od hakiranja osobnih računala ili pametnih telefona. Kršenje privatnosti vozača još je jedan mogući motiv, a napadači mogu saznati kakvu glazbu vozač sluša, kontakte iz imenika, ali i kamo se kreće, gdje radi, gdje živi i sl. Čest je motiv i financijski, odnosno napadači ili traže otkupninu za otključavanje značajki koje su, na daljinu, onemogućili, ili otvaranjem vrata i deaktiviranjem alarma, napadač može ukrasti vozilo (a najčešće ga, zatim, preprodati) [33].

Primjerice, 2021. Godine *DoppelPaymer* ransomware instaliran je na vozila azijskog proizvođača povezanih vozila, a napadači su tražili 20 milijuna dolara u zamjenu za dekriptor. Osim toga, kupci nekoliko dana nisu mogli kupovati vozila dok proizvođač nije otklonio problem [20].

Zlonamjerni softver može stvoriti širok raspon smetnji u radu upravljačkog programa. Primjeri uključuju daljinsko zaključavanje *infotainment* sustava, pojačavanje i smanjivanje glasnoće zvuka, prikazivanje pogrešnih poruka o niskom tlaku u gumama ili drugih poruka koje zahtijevaju od vozača poduzimanje hitnih radnji tijekom vožnje. Takve nagle i neočekivane radnje mogu dovesti do ljudske pogreške i uzrokovati prometne nesreće i oštetiti ugled proizvođača automobila, ali i dovesti do gubitka ljudskih života [33].

Prema Globalnom izvješću automobilske *cyber* sigurnosti iz 2022. godine dva su tipa napadača na sustave u povezanim vozilima - hakeri u bijelim šeširima i oni u crnim šeširima. 2021. godine 56.9% hakerskih napada na sustave povezanih vozila izveli su hakeri u crnim šeširima. U odnosu na 2020. godinu, kada je postotak hakerskih napada hakera u crnim šeširima iznosio 49,3%, taj se broj povećao [20].

Postoji još jedan problem koji hakerima daje prividno *opravdanje* za neovlašteni pristup sustavima povezanih vozila. Naime, tijekom 2021. zabilježeno je nekoliko slučajeva kada su pojedinci na različitim internetskim forumima postavljali pitanja i tražili upute za popravljanje vozila s namjerom izbjegavanja plaćanja ovlaštenim serviserima i proizvođačima. Kao rezultat toga, mnogi forumi i nove zajednice omogućili su korisnicima da postavljaju pitanja i primaju pomoć hakera. Takva rješenja pak nisu bila odobrena ili pregledana od proizvođača vozila, a osim toga mnogi su pojedinci bez adekvatnih znanja o softveru ili hardveru vozila (ili općenito) sami prtljali po osjetljivim instrumentima, što je stvorilo nove ranjivosti, odnosno, sigurnosne probleme tamo gdje ih prije nije bilo [20].

6. Forenzička analiza povezanih vozila

U prošlosti su sustavi u automobilu bili izolirani, a ograničene mogućnosti pristupa štitile su vozila od napadača. Međutim, suvremeni napredak i razvoj bežične komunikacije i instalacija najsuvremenijih uređaja informacijsko-komunikacijske tehnologije u vozila značajno je promijenila razina rizika od napada, ali i vrstu napada - suvremeni su napadi na vozila cyber napadi, najčešće izvedeni na daljinu, bez fizičkog pristupa [37].

Najčešće korišteni izvor digitalnih dokaza motornih vozila, EDR (također poznat kao "crna kutija") vozila, bio je uveden sredinom 1990-ih. EDR se aktivira u slučaju sudara,a bilježi 5 sekundi podataka prije sudara, kao i podatke tijekom sudara. EDR može pružiti izvor adekvatnih i kvalitetnih digitalnih dokaza za istražitelje rekonstrukcije sudara, ali često je ograničene vrijednosti u krađi vozila, prijevare ili drugim istragama povezane s vozilima. U takvim slučajevima, digitalni dokazi iz infotainment sustava vjerojatno će imati najveći utjecaj na uspjeh istrage vezane uz napade na vozila. U sadašnjosti gotovo svi proizvođači motornih vozila uključuju određenu razinu ugrađene telematike/infotainmenta, a predviđa se da će tu tehnologiju uključivati sva novo proizvedena vozila, već do 2025. godine [38].

Suvremena su vozila opremljena vrhunskim tehnološkim dostignućima i sposobna su razmjenjivati podatke s drugim vozilima, infrastrukturom, pješacima i mrežom. Osim toga, povezano vozilo sposobno je osjetiti okolinu i samoupravljati uz ograničenu ili nikakvu ljudsku intervenciju. Golema količina dostupnih podataka sustava povezanog vozila čini ga važnim izvorom digitalnih forenzičkih dokaza, budući da može pružiti detaljne (arhivirane) činjenice kao što su kao nedavna odredišta, omiljene lokacije, rute ili čak osobni podaci (npr. zapisnici poziva, popisi kontakata, SMS poruke, slike i videozapisi. Nažalost, forenzika vozila relativno je nova, u usporedbi s drugim granama digitalne forenzike, no njen se značaj neprestano ističe, a mogućnosti forenzičke analize razvijaju.Digitalna forenzika vozila pruža istražiteljima mogućnost očuvanja širokog spektra digitalnih dokaza iz motornih vozila, a sve će se više koristiti u vozilima povezana istraživanja tijekom sljedećeg desetljeća [39].

Vrijednost forenzičke istrage je u otkrivanju 5W, odnosno Tko? (engl. *Who?*), Što (engl. *What?*), Kada? (engl. *When?*), Gdje? (engl. *Where?*) i Zašto? (engl. *Why?*). Za provođenje valjane forenzičke analize povezanih vozila i otkrivanja detalja napada potrebno je:

- da vozilo sadrži digitalni mehanizam otkrivanja događaja,
- da su 5W odgovori pohranjeni u sustavu vozila te
- da su informacije o trenutnom stanju vozila pohranjene i osigurane[37].

Provedba forenzičke analize podijeljena je u dvije kategorije uživo ipost-mortem forenzička analiza. Forenzička analiza uživo je proces akvizicijetijekom rada sustava vozila. To donosi nekoliko prednosti, uključujućisposobnost prikupljanja nestabilnih podataka ili obavljanja brze analize imogućnost brze reakcije. Nedostaci su nenamjerna izmjena podataka ili manipulacijasustava, jer sam proces akvizicije može generirati podatke dnevnika

kojiprepisuje postojeće dokaze. Unutar automobilskih sustava prikupljanje DTC informacija je jedan primjer post mortem forenzičke analize. Forenzička analiza uživo je učinkovitija i pruža bogatije rezultate skupova podataka za automobilske sustave[40].

Osim toga, s obzirom na to da vozilo, ako je potrebna forenzička analiza, može biti u različitim uvjetima (uništeno, oštećeno ili netaknuto), postoje dva oblika forenzičke analize, online i offline forenzička analiza. Online forenzička analiza izvodi se korištenjem softverskih tehnika kao što je *log file* analiza. Za online forenzičku analizu, osim uređaja za povezivanje, računala za analizu i softvera za prikupljanje podataka nije potrebna nikakva dodatna oprema. Offline forenzička analiza uključuje tehnike temeljene na hardveru kao što je razdvajanje komponenti iz ECU-a ili očitavanje promjenjivih signala napona uređaji koji koriste osciloskop. Destruktivno je za vozilo jer uređaji moraju biti odvojeni od sustava u vozilu. Nadalje, offline analiza traje puno duže u usporedbi s online forenzičkom analizom. S druge strane to omogućuje prikupljanje više podataka jer se informacije čitaju izravno iz uređaja i nije potrebno prevođenje signala[40].

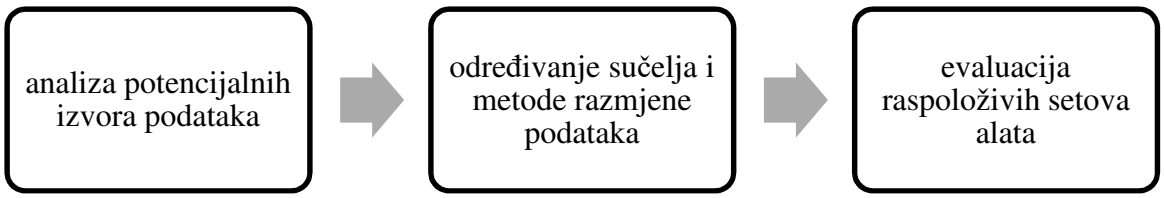
Spremnost za digitalnu forenziku ili DFR (engl. *Digital Forensic Readiness*) primijenjeno je i istraživačko područje koje se bavi planiranjem strategije digitalne forenzike. DFR planovi izrađuju se prije napada s namjerom olakšavanja i učinkovitosti forenzičke analize sustava povezanih vozila. Za implementaciju DFR-a mora se odvijati sustavan i složen rad koji obuhvaća uključivanje niza operativnih i infrastrukturnih strategija kao što su procjena rizika, edukacija osoblja, implementacija alata i sl.[39]

Elyas i sur. (2014) predložili su DFR model koji se temelji na dva čimbenika:

- sposobnostima forenzičke spremnosti i
- ciljevima forenzičke spremnosti.

Sposobnosti forenzičke spremnosti uključuju organizacijske čimbenike i samu forenzičku strategiju, dok ciljevi forenzičke spremnosti obuhvaćaju regulatornu usklađenost, upravljanje pravnim dokazima, forenzički odgovor i poslovne ciljeve.

Slika ispod prikazuje strukturu forenzičke spremnosti. Koristi se dokumentacija tijekom svakog koraka forenzičke analize. Prvo se provodi analiza potencijalnih izvora podataka, pri čemu se utvrđuju komponente u vozilu i korištene tehnologije. Općenito, većina vozila implementira slične izvore podataka. Korištene tehnologije razlikuju se ovisno o proizvođaču i modelu. Ovisno o pitanjima na koja forenzičar istrage treba odgovoriti, razlikuje se vrsta forenzičke analize. Drugi korak ove faze je određivanje sučelja i metode razmjenepodataka. Ovisno o vrsti forenzičkog očevida (uživo ili post-mortem) kao i metoda akvizicije (online i offline), primjenjive su različite metode razmjene i sučelja. Zatim, razina razvoja automobilske forenzike i dostupnost seta alata mora biti ocjenjena. Cilj evaluacije u posljednjem koraku je utvrđivanje mogućnosti ponavljanja. Za prikupljanje podataka iz vozila potrebni su hardverski i softverski alati, a funkcionalan set alata osigurava potpunu dosljednost, odgovara zahtjevima robusnosti i ponovljivosti. [40].



Slika 6.1. Struktura forenzičke spremnosti [40]

Arhitekturu DFR-a čine sljedeće komponente:

- modul atribucije napada,
- planiranje forenzičke spremnosti,
- vršitelj forenzičke strategije,
- organizator forenzičke spremnosti te
- forenzička procjena[39].

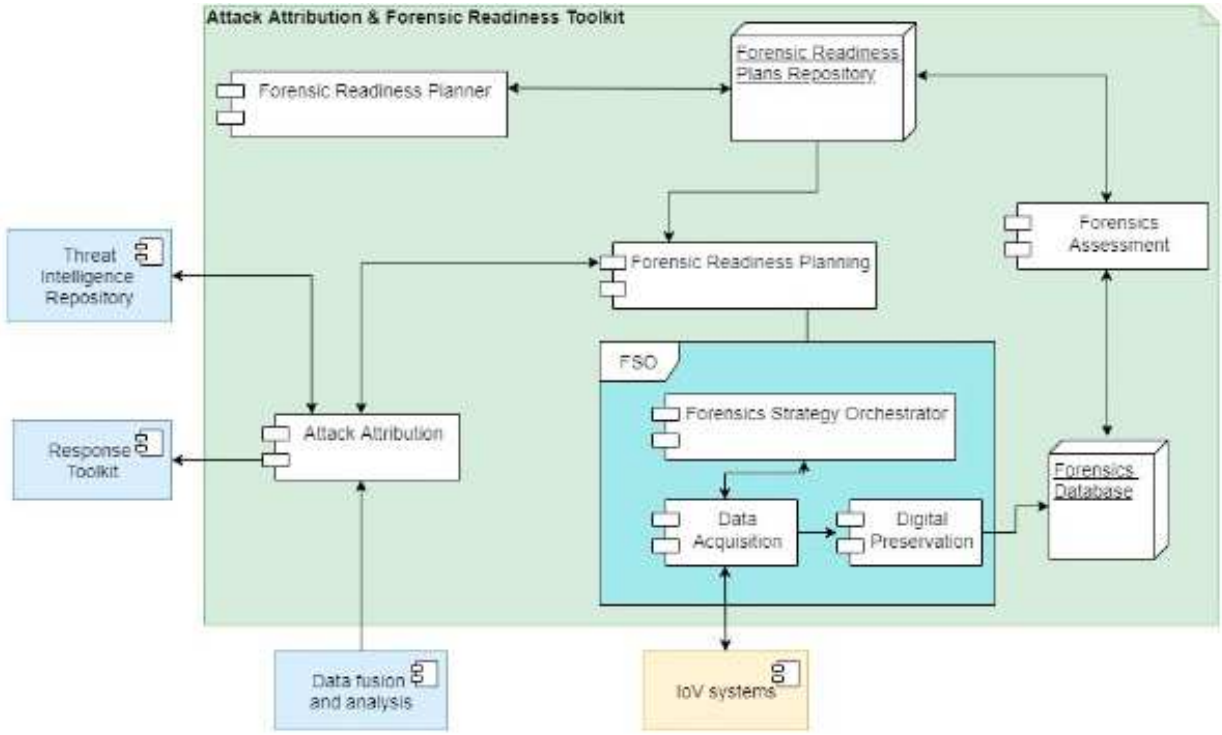
Modul atribucije napada odgovaran je za atribuciju napada. Nakon detektiranih anomalija, odnosno nakon izvršenih napada, modul procjenjuje rizik, a zatim pokreće postupak atribucije, odnosno otkrivanja vrste napada. Modul je odgovoran i za obradu informacija, identificiranje specifičnih karakteristikanapada, identificiranje pogođenih sustava vozila, moguće širenje napada i sl. [39]

Planiranje forenzičke spremnosti obuhvaća donošenje odluke o odabiru najprikladnijega plana digitalne forenzike, uz prikupljanje podataka povezanih s dokazima, nakon što je incident otkriven. Cilj je planiranja forenzičke spremnosti pripremiti se za buduće događaje i osigurati minimalne troškove odgovora, oporavkasustava i nastavak forenzičkog istraživanja [39].

Vršitelj forenzičke strategijeodgovoran je za, kako i sam naziv govori, izvršavanje aktivnosti forenzičkog plana koji je bio sastavljen u prethodnoj komponenti. Sastoji se od dva glavna podmodula: prikupljanja podatakao incidentu prema aktivnostima plana forenzike i digitalnog čuvanja podataka. Prikupljeni podaci imaju vremensku oznaku za sigurno pohranjivanje u forenzičkoj bazi podataka[39].

Planer forenzičke spremnostipruža grafičko korisničko sučelje administratorima kako bi mogli upravljati planovima i aktivnostima forenzike. To sučelje administratorima omogućava pregled, stvaranje, izmjenu ili brisanje planova i aktivnosti[39].

Forenzičku procjenučini grafičko korisničko sučelje koje pruža dvije usluge: rekonstrukciju događaja i procjenu odabrane forenzičke strategije[39]. Sve komponente DFR-a prikazuje slika ispod.



Slika 6.2. Arhitektura forenzičke analize [39]

Mnogo autora bavilo se temom važnosti forenzičke analize sustava povezanih vozila. Primjerice, istraživači Nilsson i Larson objavili su članak usredotočen na CAN. Na temelju modela napadača autori su prikazali zahtjeve za izvršenje forenzičke analize u vozilu. Da bi to bilo moguće, mreža vozila treba uključivati naprednu pohranu sustava i sustava za otkrivanje kršenja sigurnosti. Autori su izveli forenzičku analizu kroz nekoliko faza, a to su faza pripravnosti, faza raspoređivanja, faza fizičke istrage mjesta zločina, faza digitalnog očevida mjesta zločina i faza prezentacije zbivenih događaja kronološkim redom. Nilsson i Larson navode detaljne zahtjeve za pohranu podataka unutar vozila koje smatraju ključnima za sigurnost vozila [36].

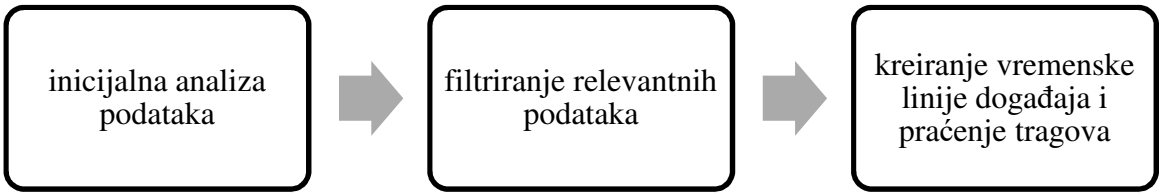
Mogući scenariji u kojima nastaje potreba za forenzičkom analizom su:

- manipulacija vozila,
- krađa vozila,
- oštećenje vozila i bijeg s mjesta nesreće te
- krađa osobnih podataka [40].

Manipulacija vozilima je modifikacija automobilskih komponenti kao što su kao ECU-ovi. Metode krađe automobila uključuju širok raspon mogućnosti od fizičkog razbijanja vozila do korištenja alata za hakiranje kao što je kopiranje digitalnih ključeva. Ako osumnjičenik izazove nesreću i udalji se s mjesta zločina, oštećenik ima poteškoća s plaćanjem popravka nastale štete te bi mu forenzička analiza mogla pomoći u otkrivanju počinitelja. Također, vrijednost forenzičke analize značajna je i u slučaju krađe osobnih

podataka jer bi se forenzičkom analizom moglo utvrditi tko je pristupio podacima i koji su točno podaci kompromitirani [40].

Struktura forenzičke analize prikazana je slikom ispod. Na početku analize količina podataka je relativna visoka. Stoga se provodi početni pregled prikupljenih podataka, odnosno rješavaju se problemi složenosti, količine ili volumena. Zatim se primjenjuju filtri za relevantni odjeljak podataka i/ili događaje. Cilj je ovog koraka odrediti dijelove podataka i/ili događaje koji se mogu koristiti kao dokazu potencijalnim kaznenim progonima. Važno je odgovoriti na postavljena pitanjaforenzičke istrage. Rješava se problem složenosti irelativno velika količina podataka svedena je samo na relevantne dijelove. Posljednji je korak stvaranje vremenskih linija i praćenje tragova. Ovo je izvedivokorištenjem posebnih alata ili ručno. Cilj je nositi se s jedinstvenim vremenskim rasporedomproblema i izgraditi sveobuhvatni i logične slijed događaja onako kako se doista i odvio [40].



Slika 6.3. Struktura forenzičke analize [40]

Rezultat forenzičke analize je rekonstrukcija događaja na temelju preciznih vremenskih oznaka. Takvi zaključci i odgovarajući rezultati bit će prihvaćeni od strane suca zbog zahtjeva robusnosti, integriteta i dosljednosti koji su, nužno, ispunjeni. Forenzičkom je analizom, dakle, moguće naknadno otkriti tko je, primjerice, ukrao određeno vozilo, a sam proces forenzičke analize koji je otkrio počinitelja daje dovoljno čvrstih materijalnih i nepobitnih dokaza koji se mogu upotrijebiti za kazneni progon krivca [40].

Prema Edmondu Locardu [41] nijedan počinitelj ne može počiniti zločin ili otići sa mjesta zločina bez ostavljanja tragova. To znači da nikakva interakcija između dva objekta nije moguća bez ostavljanja tragova, čak i u digitalnom svijetu. Digitalna forenzika bavi se prikupljanjem, restauracijom i analizom tih elektroničkih tragova. Digitalne forenzičke istrage podliježu visokim zahtjevima objektivnosti, provjerljivosti i ponovljivosti kako bi rezultati takve istrage mogli biti iskorišteni kao dokaz na sudu ili u kaznenom progonu krivca. Forenzička digitalna istraga nastoji razjasniti što se dogodilo, gdje, kada i kako, a osim toga, također je potrebno razjasniti je li incident moguće ponoviti u budućnosti. Digitalna forenzika preuzima objektivnu ulogu u razjašnjavanju tih pitanja i utvrđuje niz, kako inkriminirajućih tako i oslobađajućih digitalnih tragova [42].

Izazovi forenzičke analize i njihova relevantnost za povezana vozila prikazani su tablicom ispod.

Tablica 6.1. Izazovi digitalne forenzičke analize u industriji povezanih vozila [40]

Izazov digitalne forenzičke analize	Relevantnost za automobilsku industriju
problem složenosti	relevantno
problem različitosti	irelevantno
konzistentnost i korelacija	relevantno
kvantiteta i obujam	relevantno
jedinstvenost utvrđivanja vremenskog slijeda	relevantno

Problem složenosti opisuje porast broja složenih sustava i zamršenost prikaza podataka. Forenzička analiza skuplja je za složene sustave jer je više podataka dostupno te je teže izdvojiti, odnosno filtrirati, bitne podatke od nebitnih. Zbog sve većeg broja ECU-ova u povezanih vozilima, ovaj problem je relevantan za suvremenu automobilsku industriju. Usporedbe radi, 1994. godine u automobil je bilo ugrađeno otprilike deset ECU-ova, 2000. godine bilo ih je četrdeset, a taj se broj povećao na više od sto ugrađenih ECU-ova 2010. godine. Sve veći broj usluga mobilnosti za automobile rezultira složenijim sustavima[40].

Zbog problema raznolikosti, veliki volumeni moraju biti razdvojeni manje komade, što rezultira analizom koja oduzima manje vremena. Budući da nema velikih uređaja za pohranu u vozilima, ovaj forenzički izazov nije relevantan za automobilske sustave[40].

Dosljednost (konzistentnost) i korelacija su sveobuhvatni u digitalnoj forenzici. Potrebno je povezati više izvora podataka kako bi se proizveli upotrebljivi dokazi. Zbog velike količine ECU-a u modernim vozilima, dosljednost i korelacija značajan su izazov za automobilsku industriju povezanih vozila. Velik broj uređaja unosi puno podataka, što dovodi do poteškoća pa je istovremeno kvantiteta i obujam podataka izazov za forenzičku analizu [40].

Za procjenu redoslijeda događaja koji su se dogodili u sustavu, moraju se primijeniti vremenske oznake za različite sustave. Iako podsustavi različitih vozila različito prate, tumače i izračunavaju vrijeme, ECU-ovi s pristupom GPS-u prate trenutno GPS-vrijeme teostali ECU-i koriste ovo vrijeme kao referentnu točku, što znači da je moguće utvrditi jedinstveno vrijeme [40].

Osim opisanih izazova digitalne forenzike, nekoliko je i njenih nedostataka, a to su:

- ograničena snaga procesora,
- pristupačnost,
- sigurnosni zahtjevi te
- različiti ECU-ovi.

Snaga obrade na modernim ECU-ovima je ograničena u usporedbi s IT sustavima.Stoga forenzičkianaliza može ometati sustave u vozilu i dovesti do nenamjernih promjenadokaza. Prema zadanim postavkama, takvi uređaji ne nude pohranu podataka za kasniju forenzičku analizu te je pristup automobilskim sustavima izazovan i iz vanjske i unutarnje perspektive. Obično se vozilonalazi kod kupca ili je, u slučaju krađe, na nepoznatoj lokaciji te je dostupnost za forenzičke analitičare ograničena. Pristup ECU-ima bežičnim putem nije implementiran na većini modernih vozila. Za izvođenje ekstenzivnih forenzičke analize nekoliko ECU-a mora biti izvađeno iz vozila, a vozilo dostupno forenzičarima u, primjerice, njihovoj radioni. Vađenje ECU-ova može dovesti do smetnjii nenamjerne promjene dokaza. Sučelja kao što su OBDsu pogodnija za analizu jer su smetnje i nenamjerne promjene manje izražene nego u slučaju fizičkog vađenja ECU-ova. Automobilski sustavi dizajnirani su da ispune sigurnosne zahtjeve istandarde, a problemi se mogu pojaviti ako se ne testiraju promjene u automobilskom softveru, što dovodi do mogućeg kršenja sigurnosnih zahtjeva. Tijekom forenzikeanalize mora se osigurati da se stanje vozila ne mijenja, a to je naročito naglašeno pri izvođenju forenzičke analize uživo. Različiti ECU-ovi znače i različite tehnike forenzičke analize, a forenzičar mora biti upoznat s vozilom kako bi uspješno implementirao odgovarajuću tehniku analize vozila [40].

U svijetu forenzičke analize povezanih vozila najjača je tvrtka Berla iz SAD-a koja se bavi kreiranjem rješenja za istraživače za identificiranje, prikupljanje i analizu kritičnih informacija pohranjenih unutar vozila s namjerom otkrivanja ključnih dokaza koji određuju što se dogodilo, gdje se dogodilo i tko je bio uključen[43].

Povezana vozila prikupljaju podatke o vozilu, podatke o lokaciji i o povezanim uređajima. Podaci o vozilu uključuju zapisnik događaja povezanih s aktivnostima kao što su otvaranje vrata, promjena brzine, očitanje i mjerenje brzine, ciklusi paljenja vozila i sl. Podaci o lokaciji uključuju zapisnik puta, spremljene lokacije, aktivne ruta, česta prethodna odredišta i dr. Pohranjeni podaci o povezanim uređajima identificiraju uređaje koji su povezani putem USB priključaka, putem Bluetootha ili bežične mreže. Analiza tih pohranjenih podataka vozila dat će odgovor na ključna pitanja istražiteljima i promijeniti tijek istrage. Podaci o vozilu mogu pomoći u određivanjušto se dogodilo, gdje se dogodilo i tko je bio uključen. Otkrivanje što se dogodilo znači uvid u slijed događaja koji su se dogodili prije incidenta, identificiranje uobičajenih obrazaca i otkrivanja neobičnih događaja u vrijeme incidenta i određenje vremenskog okvira prošlih događaja. Osim otkrivanja lokacije vozila, prema podacima pohranjenim u sustavu, moguće je odrediti i koliko je dugo vozilo bilo na kojoj lokaciji. Otkrivanje počinitelja znači otkrivanje jedinstvenih identifikatora koji povezuju pojedince s određenim vozilom [43].

Za otkrivanje svega navedenog tvrtka Berla proizvela je 2014. godine iVE sustav, odnosno zbirku alata koji podržavaju istražitelje tijekom cijelog procesa forenzike vozila s mobilnom aplikacijom za identifikaciju vozila, hardverskim kompletom za prikupljanje sustava i forenzičkim softverom za analizu podataka.Osim toga, iVE sustav sadrži i upute za prikupljanje podataka, a taj proces u četiri koraka prikazuje slika ispod. Proces uključuje povezivanje iVE-a koji zatim prikuplja podatke.

Slika 6.4. Prikupljanje podataka pohranjenih u vozilu[38]

Softver iVe podržava više od 4600 različitih vozila. Najvažniji su Audi, Alfa Romeo, BMW, Chevrolet, Chrysler, FIAT, Ford, Jeep, Mercedes, Maserati, Seat, Škoda, Toyota i Volkswagen. Prema podacima sa službene internet stranice tvrtke Berla, iVE sustav koriste policijske i vojne snage, kao i različite industrije, ali dakako i fizičke osobe [43].

Ovisno o modelu vozila, veličina datoteke za prikupljanje podataka može biti veća od 25 GB. Prikupljeni podaci obično imaju vremenski žig s GPS lokacijom. Brojni podaci mogu se pohraniti i nije neuobičajeno imati više uređaja povezanih s jednim sustavom, odražavajući tko može povezivati svoj uređaj s vozilom. Takvi zapisi mogu pružiti ključni uvid u dokaze o napadaču na povezana vozila kada nema drugih izvora dokaza i tragova [38].

iVE je forenzički softverski alat napravljen za analizu podataka vozila. Sustav se sastoji od zbirke hardverskih i softverskih alata koji pomažu istražitelju u istraživanju podataka o vozilu. Moćan iVE softver omogućava brzu analizu dobivenih informacija. Te su informacije opširne i detaljne, a uključuju informacije poput odgovora na sljedeća pitanja: Kada i gdje su upaljena svjetla? Koja su se vrata otvarala i zatvarala i na kojim mjestima? Gdje je bilo vozilo u trenutku povezivanja Bluetooth uređaja?

iVe može izvući fizičke i logičke podatke iz infotainment i telematskih jedinica putem OBD II priključka, USB priključaka unutar vozila i/ili posebnih dijagnostičkih priključaka na navigacijskome sustavu. Metoda ekstrakcije i analize su zaštićene – dakle, nije potpuno jasno kako se izvlače informacije i koje datotečne sustave iVe podržava. U ovom trenutku iVe

podržava samo mali broj europskih vozila poput BMW-a i Volkswagena. Na primjer, u BMW QNX datotečnom sustavu, alat iVE se može koristiti se za izdvajanje logičkih informacija preko OBD II priključka ili USB priključka spojenog na infotainment sustav [44].

Primjerice, od 2007. Ford je uveo četiri sustava s različitim vrstama podataka dostupnih korištenjem iVE alata, a to su:

- Ford Navigation Radio,
- Ford Sync 1 objavljen 2007. godine (trenutačno dostupan u nekim novim modelima vozila),
- My Touch Ford® od 2012. do 2015. (poznat i kao Ford Sync 2) te
- Ford Sync 3 objavljen 2015. i isporučen u nekim novim modelima vozila[38].

Usporedba količine i vrste podataka dostupnih iz sustava SYNC® 1 i SYNC® 3 daje jasne podatke o tome da će neki sustavi sadržavati značajno više informacija nego drugi sustavi. Na primjer, podaci pohranjeni i dostupni od SYNC® 1 mogu sadržavati korisne informacije kao što su kao jedinstvene Bluetooth adrese za povezane telefone, zapisnike telefonskih poziva (dolazne, odlazne i propuštene) i SMS tekstualne poruke.SYNC® 1 ne pohranjuje navigacijske podatke vozila, dok SYNC® 3 može sadržavati jedinstvene Bluetooth i Wi-Fi adrese za povezane uređaje; telefonske zapisnike (dolazni, odlazni i propušteni pozivi) te mnoge vrste vremenskog žiga (s GPS lokacijom) za događaje vozila, kao i informacije je li Apple CarPlayTM bio omogućen, je li Android AutoTM bio omogućen, informacije o otvaranju i zatvaranju vrata vozila, upozorenja o ometanju vozača, podatke o snažnom ubrzanju, oštrom kočenju, podatke iz medija, brojač kilometara, USB veze i Wi-Fi veze. Osim toga, SYNC® 3 može uključiti podatke o navigaciji kao što su lokacije, rute, zapisi puta i karotaže brzine. Osim podataka pohranjenih u vozilu, neki podaci vjerojatno se prenose iz vozila i pohranjuju na daljinu u "oblaku" (prikupljaju ga proizvođači, osiguravajuća društva ili druge treće strane)[38].

Tako prikupljeni podaci postaju sve vrjedniji izvor digitalnih dokaza. Mogućnost pristupa ovim podacima može varirati ovisno o tome tko traži podatke i za koju svrhu. Vrlo je vjerojatno da će osiguravajuće društvo moći podijeliti informacije sa svojim internim istražiteljima. Osim toga, podaci mogu biti dostupni tijelima za provedbu zakona korištenjem odgovarajućih sudskih ovlaštenja i zahtjeva za nalog za izvođenje telekomunikacije i sl. [38].

Istraživanje o mogućnostima oporavka i pristupanju informacija vozila proveli su Whelan i sur. 2018. godine. Konkretno, usporedili su mogućnosti iVE sustava na dva automobile Dodgeu Dart iz 2013. godine te Toyoti Highlander iz iste godine[45].

Faze protokola prikupljanja informacije prikazane su i objašnjene tablicom ispod.

Tablica 6.2. Protokol prikupljanja informacija iz povezanih vozila [45]

Faza prikupljanja podataka	Prikaz faze	Aktivnosti faze
Baseline	otkrivanje podataka u sustavu	prikupljanje podataka u sustavu
Unpair/"Un-sync"	određivanje jesu li i koji podaci nepovratni uklanjanjem telefona	prikupljanje podataka u sustavu
Brisanje osobnih podataka	određivanje jesu li i koji podaci nepovratni brisanjem osobnih podataka	prikupljanje podataka u sustavu

U istraživanju je vizualnim pregledom Dodgea Dart uočeno da postoje tri prethodno uparena uređaja navedena na zaslonu sustava. Osim imena uređaja, nije bilo dodatnih podataka o korisniku dostupnih na zaslonu infotainment sustava. Nakon analize informacija, istraživači su vidjeli da nema priključenih uređaja, SMS poruka, poziva, zapisa u dnevniku ili kontakata identificiranih i prikupljenih softverom iVe. Jedina relevantna informacija dobiven iz sustava bio je popis adresa s lokacija navedenih u sustavu. Te su adrese također navedene s pripadajućim geografskim podacima (geografska širina i dužina) [45].

Vizualnim pregledom infotainment sustava Toyota automobila uočeno je da su tri uređaja navedena kao uparena sa sustavom. Osim imena uređaja, nisu bile dostupne korisničke informacije sa zaslona infotainment sustava. Daljnjom analizom dobivenih osnovnih podataka, navedeno je 13 uređaja, od kojih su 3 ona prvotno uočena. Za svaki od ta 3 uređaja bilo je stotine kontakata i zapise poziva koji su prikupljeni iVe sustavom. Primijećeno je da bi zapisnici poziva mogli biti stari tri godine, a od povezanih uređaja jedan je imao navedenu samo verziju telefona, a druga dva su odavala i međunarodne identitete dok je jedan naveo čak i korisnički jedinstveni Apple ID broj. Za ostalih 10 uređaja pronađeni su podaci o 22 medijske datoteke, kao i više kontakata i zapisnike poziva. Informacije o 22 medijske datoteke bile su s 2 različita uređaja (11 sa svakog uređaja), a sve su navedene kao audio datoteke [45].

Uspoređujući informacije izvučene iz svakog sustava, jasno je da su forenzički relevantniji podaci dobiveni iz Toyotinog automobila. Toyota sustav osigurava uređaje, kontakte, zapise poziva, audio datoteke i lokacije, dok sustav Dodgea pruža samo podatke o lokaciji. Tablica u nastavku daje usporedbu oporavljenih informacija iz svakog od dva istraživana vozila, kao i ukupni broj svake oporavljene vrste .

Tablica 6.3. Usporedba prikupljenih informacija s infotainmenta iVE sustavom [45]

Sustav	2013 Dodge® Dart Limited	2013 Toyota™ Highlander Limited
Pronađene informacije	Uređaji na zaslonu	Uređaji i kontakti
	Lokacije i adrese	Povijest poziva, audio datoteke, lokacije i adrese
Ukupan broj zapisa	tri uređaja	13 uređaja
	53 lokacije	1,347 kontakata
	50 ruta	603 poziva
		22 medijske datoteke
		18 poziva

Istraživači su primijetili da proces prikupljanja podataka (sustavom bez blokatora) može unijeti promjeni u pregledavani sustav vozila, ali zaključili su da su gotovi svi podaci dobiveni iz infotainment sustava označeni su vremenom, što omogućuje analitičaru da utvrdi na što je utjecao proces prikupljanja podataka i koje je informacije dodao sustav iVE. Čak iako su zapisi napravljeni u sustavu, to ne umanjuje mogućnost da se ove vrste digitalnih dokaza koriste na sudu. Budući da je forenzika vozila novo područje, ono tek treba dosegnuti svoj puni uspjeh potencijal, pa tako i razvoj mnogo sustava za forenziku, osim iznad opisanog Berlinog iVE sustava.

7. Zaključak

Povezano vozilo je svako vozilo koje ima mogućnost komunikacije s uređajima u blizini putem bežičnih mreža, a koncept povezanih vozila odnosi se na aplikacije, usluge i tehnologije koje povezuju vozilo s njegovim okruženjem. Povezano je vozilo ono vozilo u kojem postoji uređaj za povezivanje s drugim uređajima unutar istog vozila i/ili uređaja te mrežom, aplikacijama i uslugama izvan vozila. Funkcije tih uređaja povezanih vozila su osiguravanje sigurnost u prometu, olakšavanje parkiranja vozila, pomoć na cesti, dijagnostika stanja vozila na daljinu, autonomnost vozila, i dr.

Atraktivnost sustava povezanih vozila za vozače i razvoj automobilske industrije prema masovnoj proizvodnji povezanih vozila označava i razvoj komunikacijskih protokola vozila, od kojih su trenutno u upotrebi: CAN, LIN, AE, FlexRay i MOST. Ti se protokoli razlikuju prema brzini slanja informacija, broju čvorova, duljini mreže, načinu slanja poruka, financijskim troškovima i dostupnosti.

Povezivanje vozila s vanjskim okruženjem označava i povećavanje rizika od*cyber* napada na vozilo.Različiti cyber napadi izvršeni su i kao testiranje mogućnosti i razine ranjivosti vozila (hakeri u bijelim šeširima), ali i kao zlonamjerni napadi različitih motiva poput kršenja privatnosti vozača, krađe vozila, ozljeđivanje vozača i putnika, ometanje prometa i sl. (hakeri u crnim šeširima). Mnogo je mogućih načina za neovlašteni pristup sustavu povezanih vozila, a usluge povezanih vozila koje su posebno osjetljive, odnosno rizične, za hakerski napad su: lokator vozila, daljinsko otključavanje i pokretanje te praćenje stanja voznog parka.

U slučaju napada, ali često i prije samoga napada, s namjerom zaštite vozila, provodi se detaljna forenzička analiza. Forenzička je analiza iznimno korisna jer, kao što je i povijest razvoja povezanih vozila pokazala, jednom otkrivena ranjivost sustava nužno se ažurira i osnažuje u procesu daljnje proizvodnje vozila.

8. Popis literature

1. Uhlemann, E. Introducing Connected Vehicles [Connected Vehicles], *IEEE Vehicular Technology Magazine*; 2015 (3).
2. Martin, T. Commuting to work: Results of the 2010 general social survey, *Statistics Canada*; 2011 (8).
3. Brian, M. Commuting in United States,*Canada's Emission Trend*, 2012.
4. Letter, C. E. L. Efficient control of fully automated connected vehicles at, Transportation Research Part C; 2017 (4).
5. Yang D. G., Jiang K., Zhao D. Intelligent and connected vehicles: Current status and future perspectives, *Sci China Tech Sci*, 2018 (10).
6. *Fue Loyal*, Preuzeto s: https://www.fueloyal.com/what-is-connected-vehicle-and-history-of-connected-vehicles/. [Pristupljeno: 8. 8. 2022.].
7. *Auto Connected Car News*, Preuzeto s: https://www.autoconnectedcar.com/definition-of-connected-car-what-is-the-connected-car-defined/. [Pristupljeno: 8. 8. 2022.].
8. El-Rewini, Z. E. R., Sadatsharan, K., Selvaraj, D. F., Plathottam, S. J., Ranganathan, P., Cybersecurity challenges in vehicular communications, *Vehicular Communications*, 2020 (12).
9. Jadaan, K., Zaeter, S., Abukhalif, Y., Connected Vehicles: an Innovative Transport Technology, *Procedia Engineering*, p. 641 – 648, 2017.
10. Ishak, M. K., Khan, F. K., Unique Message Authentication Security Approach based Controller Area Network (CAN) for Anti-lock Braking System (ABS) in Vehicle Network, *Procedia Computer Science*, 2019 (11).
11. Wilmshurst, T. Designing Embedded Systems with PIC Microcontrollers Principles and Applications, *Elsevier Ltd*, 2010.
12. Ibrahim, D. PIC Microcontroller Projects in C Basic to Advanced, Elsevier Ltd, 2014.
13. Zubair, M. *Inspired Hobbyist*, Preuzeto s: https://inspiredhobbyist.org/automotive-ethernet-what-is-driving-force-to-the-adaption-of-in-vehicle-networks-to-ethernet/. [Pristupljeno: 9. 8. 2022.].
14. Nilsson, D. K., Larson, U. E., Picasso, F., Jonsson, E. A First Simulation of Attacks in the Automotive Network Communications Protocol FlexRay, *Proceedings of the International Workshop on Computational Intelligence in Security for Information Systems CISIS'08. Advances in Soft Computing*, vol 53., Berlin, 2009.
15. Tigadi, V. EDN, Preuzeto s: https://www.edn.com/build-simple-and-inexpensive-flexray-nodes/. [Pristupljeno: 9. 8. 2022.].
16. Sumorek, A. B. M. New elements in vehicle communication, Teka. *Commission of motorization and energetics in agriculture*, 2012.
17. Sheehan, B., Murphy, F., Mullins, M., Ryan, C. Connected and autonomous vehicles: A cyber-risk classification, *Transportation Research*, 2019 (11).
18. International Fleet World, Preuzeto s: https://internationalfleetworld.com/connect-with-safety/. [Pristupljeno: 16. 8. 2022.].

19. Nash, L., Boehmer, G., Wireman, M., Hilaker, A., Securing the future of mobility Addressing cyber risk in self-driving cars and beyond,*Deloitte*, 2017 (4).
20. Upstream, Global Automotive Cybersecurity Report,*Upstream Security Ltd*., 2022.
21. Pham, M., Xiong, K.*A survey on security attacks and defense techniques for connected and autonomous vehicles*,Elsevier,2021.
22. Parkisnkon, S., Ward, P., Wilson, K., Miller, J., Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges, *IEEE Transactions on Intelligent Transportation Systems*, pp. 1-18, 2017 (3).
23. Cyber Talk, Preuzeto s: https://www.cybertalk.org/2022/05/19/new-bluetooth-hack-demonstrated-on-tesla-affects-millions-of-devices/. [Pristupljeno: 15. 8. 2022.].
24. Bryans, J., Shaik, S., Cheah, M., TU-Automotive Hacks and Threats Report 2016,*TU Automotive Cyber Security*, 2016 (11).
25. Upstream, Preuzeto s: https://upstream.auto/blog/how-to-mitigate-keyless-entry-attacks/. [Pristupljeno: 15. 8. 2022.].
26. Eiza, M. H., Ni, Q., DRIVING WITH SHARKS Rethinking Connected Vehicles with Vehicle Cybersecurity, *IEEE vehicular technology magazine,* 2017 (6).
27. Daimi, K., Saed, M., *Securing Tire Pressure Monitoring System*, AICT 2018: The Fourteenth Advanced International Conference on Telecommunications, 2018.
28. Roufa, I., Miller, R., Mustafa, H., Tayloer, T., Oh, S., XU, W., Gruteser, M., Trappe, W., Seskar, I., Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study, *The 19th USENIX conference on Security* (USENIX Security'10), Washington, DC, 2010.
29. Qaconsultants, Preuzeto s: https://qaconsultants.com/blog/connected-and-autonomous-vehicle-cybersecurity-sensor-attacks/. [Pristupljeno: 14. 8. 2022.].
30. Perfetto, I. Cosmos Magazine, Preuzeto s: https://cosmosmagazine.com/news/tricking-driverless-car-sensors/. [Pristupljeno: 25. 8. 2022.].
31. Khatri, N., Shrestha, R., Nam, S., Y., Security Issues with In-Vehicle Networks, and Enhanced Countermeasures Based on Blockchain, *Electronics*, 2021 (4).
32. IotaSmart, Preuzeto s: http://iotasmart.com/blog/security-features-connected-cars/. [Pristupljeno: 16. 8. 2022.].
33. Zhang, T., Antunes, H., Aggarwal, S., Defending Connected Vehicles Against Malware: Challenges and a Solution Framework,*IEEE Internet of Things Journal*, 2014 (2).
34. Hoppe, T., Dittman, J. S., Replay Attacks on CAN Buses: A simulated attack on the electric windowlift classified using an adapted CERT taxonomy, *Proceedings of the 2nd Workshop on Embedded SystemsSecurity* (WESS), Salzburg, 2007.
35. AUTOCRYPT, Preuzeto s: https://autocrypt.io/who-launch-cyberattacks-on-connected-cars-and-why/. [Pristupljeno: 4. 9. 2022.].
36. Hayton, R. Trustonic. Preuezeo s: https://www.trustonic.com/opinion/who-would-want-to-hack-your-car/. [Pristupljeno: 4. 9. 2022.].
37. Nilsson, D. K., Larson, U. E., Conducting Forensic Investigations of Cyber Attacks on Automobile In-Vehicle Networks, *Ernational Journal of Digital Crime and Foren*, 4-6 2009.

38. Eoin, A. B.Preuezto s: https://abforensics.com/wp-content/uploads/2019/02/INTERPOL-4N6-PULSE-IssueIV-BATES.pdf. [Pristupljeno: 3. 9. 2022.].
39. Alexakos, C., Katsini, C., Votis, K., Lalas, A., Tzovaras, D., Serpanos, D., Enabling Digital Forensics Readiness for Internet of Vehicles, *Transportation Research Procedia*, 2020 (9).
40. Klaus Gomez Buquerin, K. *Analysis of Digital Forensic Capabilities on State-of the art Vehicles*, Ingolstadt: Technical University Ingolstadt, 2020.
41. Locard, E.*Die Kriminaluntersuchung und ihre wissenschaftlichen Methoden*, Berlin: Berliner Kameradschaft, 1930.
42. Ebbers, S., Ising, F., Saatjohann, C., Schinzel, S., *Grand Theft App: Digital Forensics of Vehicle Assistant Apps*, The 16th International Conference on Availability, Reliability and Security, Beč, 2021.
43. Berla, Preuezto s: https://berla.co/. [Pristupljeno: 3. 9. 2022.].
44. Le Khac, N. A., Jacobs, D., Nijhoff, J., Bertens, K., Choo, K. K. R.Preuzeto s: https://www.sciencedirect.com/science/article/abs/pii/S0167739X17322422. [Pristupljeno: 3. 9. 2022.].
45. Whelan, C. J., Sammons, J., McManus, B., Fenger, T. W., Retrieval of Infotainment System Artifacts from Vehicles Using iVE, *Journal of Applied Digital Evidence*, 2018.
46. Shladover, S. E. Connected and automated vehicle systems: Introduction and overview, *Journal of Intelligent Transportation Systems* , 2017 (5).
47. Greenberg, A. WIRED, Preuezeto s: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. [Pristupljeno: 25. 8. 2022.].

9. Popis kratica

ADAS (*Advanced Driver-Assistance Systems*) sustav napredne asistencije vozačima

AE (*Automotive Ethernet*) automobilski ethernet

CAN (*Controller Area Network*) protokol kontrolne mreže

DFR (*Digital Forensic Readiness*)spremnost za digitalnu forenziku

ECU (*Electronic Control Units*) elektronički kontrolirana jedinica

GPS (*Global Positioning Systems*) navigacijski sustav

ITS (*Intelligent Transportation Systems*) inteligentni sustav prijevoza

IVI (*In-vehicle infotainment*)infotainment sustavi u vozilu

LiDAR (*Light Detection and Ranging*) sustav daljinskog očitavanja svjetlosnim valovima

LIN (*Local Interconnect Network*) lokalna interkonekcijska mreža

LTE (*Long-Term Evolution*) dugoročna evolucija

MOST (*Media Oriented Serial Transport*) sustav usmjeren na prijenos informacija

NVD (*National Vulnerability Database*) nacionalna baza podataka ranjivosti

OBD (*On-Board Diagnostics*) samodijagnostika vozila

SAE (*Society of Automotive Engineers*) društvo automobilskih inženjera

TARA (*Threat Assessment and Remediation Analysis*) procjena prijetnji i analiza sanacije

TPMS (*Tire Pressure Monitoring System*) sustav upozorenja za mjerenje tlaka zraka u gumama

USRP (engl. *Universal Software Radio Peripheral*) javna softverska platforma USRP

10. Popis slika

11. Popis tablica

Nisu pronađeni unosi u tablici slika.

12. Popis grafova

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je diplomski rad
(*vrsta rada*)
isključivo rezultat mojega vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju upotrijebljene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedopušten način, odnosno da je prepisan iz necitiranog rada te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu diplomskog rada pod naslovom Analiza potencijalnih točaka za neovlašteni pristup povezanim vozilima, u Nacionalni repozitorij završnih i diplomskih radova ZIR.

Student/ica:

U Zagrebu, 05.09.2022.

(ime i prezime, *potpis*)