Značajke informacijsko - komunikacijske sigurnosti autonomnih vozila

Komušar, Ivan

Master's thesis / Diplomski rad

2021

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:119:937247

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Ivan Komušar

RAČUNALNA SIGURNOST AUTONOMNIH VOZILA

Diplomski rad

ZAGREB, 2021.

SVEUŠILIŠTE U ZAGREBU FAKULTET PROMETNIH ZNANOSTI POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 28. travnja 2021.

Zavod: **Zavod za inteligentne transportne sustave**

Predmet: **Računalna sigurnost**

DIPLOMSKI ZADATAK br. 6306

Pristupnik: **Ivan Komušar (0135231275)**

Studij: Inteligentni transportni sustavi i logistika

Smjer: Inteligentni transportni sustavi

Zadatak: **Značajke informacijsko - komunikacijske sigurnosti autonomnih vozila**

Opis zadatka:

Brzi tehnološki napredak doveo je do pojave autonomnih vozila, mebutim njihova društvena prihvatljivost i sigurnosni problemi predstavljaju značajan izazov kao u tehničko-tehnološkom tako i u zakonodavnom te ostalom smislu. Navedeno područje potrebno je opisati kroz društvene zahtjeve i pravne okvire autonomne vožnje, tehničko-tehnološke koncepte autonomnih vozila i autonomne vožnje te sigurnosne aspekte autonomne vožnje i analizu strategija uvobenja autonomnih vozila.

Mentor: Predsjednik povjerenstva za diplomski ispit:

doc. dr. sc. Pero Škorput

Sveučilište u Zagrebu

Fakultet prometnih znanosti

DIPLOMSKI RAD

RAČUNALNA SIGURNOST AUTONOMNIH VOZILA

CYBER SECURITY OF AUTONOMOUS VEHICLES

Mentor: doc. dr. sc. Pero Škorput

Student: Ivan Komušar

JMBAG: 0135231275

Zagreb, kolovoz 2021.

Zahvale

Zahvaljujem svojem mentoru doc. dr. sc. Pero Škorput na uputama, strpljenju i pomoći tijekom pisanja ovog rada. Zahvaljujem se svim profesorima i asistentima na znanju koje su mi prenijeli tijekom studiranja. Također zahvaljujem svojoj obiteljii, prijateljima i svima koji su mi pružili potporu tijekom mojeg studiranja.

Sažetak

Naslov: Računalna sigurnost autonomnih vozila

Ubrzanim razvojem tehnologije, te sve većom urbanizacijom, dolazi do razvoja prometnog sustava što dovodi do sve većih gužva na prometnicama, a samim time i smanjenja razine usluga koje promet pruža. Kako bi se smanjila zagušenja, zagađenja i ostali problemi u prometu, pribjegava se novim prometnim rješenjima, te dolazi do pojave "ITS- a", odnosno inteligentnih prometnih sustava. Jedno od mnogih rješenja koje ITS nudi za rješavanje takvih prometnih problema su autonomna vozila. Autonomna vožnja dijeli se na pet razina koje ovise o tome koliko intervencije vozača zahtjeva vožnja. Smatra se da će korištenje autonomnih vozila doprinjeti smanjenju zagušenja, zagađenja, te povećati sigurnost i udobnost prilikom putovanja. Osim pozitivnih stvari koje nam autonomna vozila nose, postoji i određena zabrinutost u vezi računalne sigurnosti takvih vozila. U ovom radu opisani su elementi autonomnog vozila,te njihova potencijalna ranjivost, odnosno kako se one mogu iskoristiti.

Ključne riječi: Inteligentni transportni sustavi, autonomna vozila, autonomna vožnja, računalna sigurnost

Abstract

Title: Cyber security of autonomous vehicles

Accelerated development of technology, and increasing urbanization, leads to the development of the transport system, which leads to increasing congestion on the roads, and thus reduce the level of services provided by transport. In order to reduce congestion, pollution and other traffic problems, new traffic solutions are resorted to, and the emergence of "ITS", or intelligent transport systems. One of the many solutions that ITS offers to solve such traffic problems are autonomous vehicles. Autonomous driving is divided into five levels that depend on how much driver intervention the driving requires. It is believed that the use of autonomous vehicles will contribute to reducing congestion, pollution, and increase safety and comfort when traveling. In addition to the positive things that autonomous vehicles bring us, there are also some concerns about the cyber security of such vehicles. This paper describes the elements of an autonomous vehicle, and their potential vulnerability, ie how they can be exploited.

Keywords: Intelligent transport systems, autonomous vehicles, autonomous driving, cyber security

SADRŽAJ

1. Uvod

U današnjem svijetu u kojem se stvari brzo mijenjaju, gradovi brzo i neprestano rastu, urbani centri bave se rekordnom razinom prometa i zagađenja. Ljudi na vodećim pozicijama prepoznali su sve veću urbanizaciju kao jedan od ključnih trendova 21. stoljeća. Ovaj rast također uzrokuje pomak s individualnog vlasništva nad vozilom na korištenje mogućnosti zajedničke mobilnosti kao što su usluge javnog gradskog prijevoza, te dijeljenja prijevoznog sredstva sa drugim ljudima.

Većina naše infrastrukture izgrađena je kako bi zadovoljila potrebe pojedinačno rabljenih vozila. Međutim, većina tih vozila miruje oko 95% vremena. Kao rezultat toga, čak 30% nekretnina u centru grada posvećeno je parkiranju. Ako se pravilno primjene, nove tehnologije mogu omogućiti rješenja koja pomažu gradskim prometnim sustavima da poboljšaju kvalitetu života za sve, ali ove tehnologije mobilnosti i usluge u gradu ili četvrti neće riješiti sve postojeće izazove i čak ih mogu pogoršati. Kao rješenje većine problema vezanih uz promet nade se polažu u autonomna vozila (AV).

Da bismo razumjeli potencijalne načine uporabe autonomnih vozila, prvo moramo o njima razmišljati na drugačiji način od načina na koji trenutno razmišlja većina korisnika automobila, kamiona i drugih vozila. Taksiji su originalna usluga "na zahtjev" jer je za to potreban samo pokret rukom ili poziv mobilnim uređajem da bi se taksi "stvorio" pred vama. Uz dostupnost novih tehnologija takva usluga dovodi se na višu razinu, odnosno to je smjernica u kojem smjeru bi razvoj autonomnih vozila trebao ići. U budućnosti se očekuju usluge prijevoza i dijeljenja automobila koje nude još više mogućnosti za kupce. Autonomna vozila mogu poboljšati ove usluge i proširiti njihovu dostupnost i pristupačnost - s posebnim naglaskom na djelovanje u područjima u kojima usluge prijevoza nisu zadovoljene. Također mogu biti podrška za ljude koji ne mogu sami voziti zbog starosti ili invalidnosti.

Autonomno vozilo može raditi bez ljudske kontrole i ne zahtjeva nikakvu ljudsku intervenciju. Suvremena autonomna vozila mogu osjetiti svoje lokalno okruženje, klasificirati

različite vrste objekata koje otkriju, interpretirati osjetilne informacije za identificiranje odgovarajućih navigacijskih staza poštujući pravila prijevoza. Značajan napredak postignut je u odgovarajućem odgovoru na neočekivane okolnosti u kojima se može dogoditi zastoj u voznim sustavima ili se neki medij u vanjskom okruženju ne ponaša onako kako su predviđali interni prototipi. Za uspješnu autonomnu navigaciju u takvim situacijama značajno je kombiniranje različitih tehnologija iz različitih disciplina koje obuhvaćaju informatiku, strojarstvo, elektroniku, elektrotehniku i kontrolno inženjerstvo I tako dalje.[1]

Jedan od glavnih problema za koje bi rješenje trebala biti autonomna vozila su prometne nesreće. Svake godine životi otprilike 1,35 milijuna ljudi se prekinu kao posljedica prometne nesreće. Između 20 i 50 milijuna ljudi pretrpi smrtne posljedice, a mnogi imaju trajne ozljede kao posljedice nesreće. Ozljede u cestovnom prometu uzrokuju znatne ekonomske gubitke pojedincima, njihovim obiteljima i cijeloj naciji. Ti gubici nastaju zbog troškova liječenja, kao i zbog gubitka produktivnosti za one koji su nastradali ili onesposobljeni zbog ozljeda, kao i za članove obitelji kojima je potrebno prilagoditi posao ili školu kako bi se brinuli o ozlijeđenima. Sudari u cestovnom prometu koštaju većinu zemalja oko 3% njihovog bruto domaćeg proizvoda.[2]

Smatra se da će se uvođenjem autonomnih vozila broj prometnih nesreća drastično smanjiti zbog povećanja sigurnosti i brže reakcije koje pružaju takva vozila u usporedbi sa čovjekom. Također, očekuju se smanjenja zagušenja prometa i na taj način povećanje kapaciteta ceste budući da bi autonomna vozila vodila ka smanjenju potreba za sigurnosnim prazninama i boljem protoku prometa, odnosno upravljanju prometnom mrežom.

Autonomna vozila pružaju izvrsne prednosti, ali postoje određene mane. Iako industrija automobila to negira, vjeruje se da će implementacija autonomnih vozila dovesti do smanjenja radnih mjesta vezanih uz vožnju. Također, mnogo ljudi uživa vozeći automobil i teško Im je oduzeti tu mogućnost i povlasticu pa je to jedan od izazova koji valja riješiti. Autonomni automobili predstavljaju izazove u interakciji s vozilima kojima upravlja čovjek, a nalaze se na istoj

[1] Deshpande, Pawan. "Road Safety and Accident Prevention in India: A review." U: International Journal of Advanced Engineering and Technology. Travanj- Lipanj/ 2014.str.68

[2] World healt organization “Road traffic injuries”. https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries

ruti. Još jedan izazov je onaj tko treba odgovarati za oštećenja/nesreće - tvrtka za proizvodnju automobila, vlasnik automobila ili vlada, odnosno državni organi.

Zbog toga, donošenje i uspostava zakonskog okvira te uspostava vladinih propisa, a nakraju i provedba istog od velike su važnosti, odnosno veliki su problem oko kojeg je potrebna suglasnost više “stakeholdera”. Pouzdanost softvera je također upitna zbog mogućih napada hakera, te preuzimanja kontrole nad vozilom od strane treće osobe koja bi mogla ugroziti sigurnost putnika i komunikaciju između vozila, odnosno povećati rizik od terorističkih napada. Osim preuzimanja vozila, eksploziv bi bilo moguće utovariti u vozilo te unijeti lokaciju te tako bez previše rizika ugroziti živote milijuna ljudi. Uz to moguće bi bilo vozilo koristiti za različite kriminalne radnje pa je potrebno detaljno i uz puno pažnje smisliti rješenja za sve te potencijalno opasne radnje.

Cilj ovog diplomskog je prikazati problematiku računalne sigurnosti autonomnih vozila i predstaviti potencijalne opasnosti te kako ih otkloniti odnosno izbjeći. Ovaj rad je sastavljen od 6 poglavlja. U uvodnom poglavlju dan je opci pregled tematike te je predstavljen cilj i struktura rada. U drugom poglavlju opisana je računalna sigurnost u prometu, razvoj informacijsko komunikacijske tehnologije I mogući napadi na vozila I sustav. Treće poglavlje odnosi se na autonomna vozila te način na koji ista rade, odnosno skeniraju svoju okolinu. U četvrtom poglavlju opisani su zahtjevi koji su stavljeni pred autonomna vozila i koje ista moraju zadovoljiti. Peto poglavlje odnosi se na procjenu rizika od cyber napada na autonomna vozila. U zadnjem poglavlju iznesen je zaključak prema prethodnim poglavljima.

2. Računalna sigurnost u prometu

Pojavom "pametnih gradova" dolazi do veće povezanosti između različitih sektora iz različitih domena aktivnosti što dovodi do bržeg tehnološkog razvoja, te do povećane uloge i sve većeg oslanjanja na informacijske i komunikacijske tehnologije u raznim procesima.

Informacijsko- komunikacijska tehnologija

Inteligentni transportni sustavi integriraju informacijsku i komunikacijsku tehnologiju (ICT) s transportnim inženjeringom kako bi omogućio bolje planiranje, dizajniranje, upravljanje, održavanje prometnog sustava, što zauzvrat značajno doprinosi poboljšanju učinkovitosti i radu takvih mreža.[3]

Takvi sustavi rade na principu dohvaćanja, obrade i razmjene podataka, a njihova integracija omogućuje "Inteligentni prometni sustav" kakav danas poznajemo i koji svakim danom postaje sve napredniji. U takvom sustavu gdje su umreženi fizički uređaji, komunikacijske mreže i centralni poslužitelji, usluge postaju optimizirane do određenog stupnja automatizacije. Usprkos tome što takav spoj mrežne tehnologije, fizičke infrastrukture, pametnih uređaja i vozila stvara veliko poboljšanje i mogućnosti poboljšanja usluga u prometu, također stvara i moguće nove potencijalne prijetnje i probleme. Jedan od takvih potencijalnih problema je računalna sigurnost prometne mreže koja u prošlosti nije bila podložna takvim prijetnjama. Štoviše, prometna mreža postaje primamljiva kao meta takvih napada koje ne stvaraju samo prometne probleme i gubitke već i ekonomske, gospodarske, te potencijalno ugrožavaju sigurnost i živote građana.

Ovo povećanje rizika računalne sigurnosti za IPT stvara nove ciljeve koje treba ispuniti. Tu spadaju:

[3] Bosnjak, I.; Inteligentni transportni sustavi 1. Sveučilište u Zagrebu, Fakultet prometnih znanosti, Zagreb, 2006.

- Identificiranje kritičnih ITS sredstava i s njima povezanih prijetnji
- Identificiranje dobrih praksi u kibernetičkoj sigurnosti koje mogu riješiti ove prijetnje i povećati cyber otpornost ITS operatora
- Koherentna strategija i politika pristupa koja obuhvaća sve "stakeholdere" povezane s ITS-om u okruženju “pametnog” grada

Funkcionalnost autonomnih vozila ovisi o međusobnoj povezivosti tehnologija koje razmjenjuju informacije putem bežične komunikacije na mreži. Mreže su ranjive na zlonamjerni softver, viruse i distribuirane napade koji mogu uzrokovati uskraćivanje usluge, između ostalog. Hakiranje uzrokuje značajne povrede podataka, krađu kritičnih podataka ili potpunu eksploataciju ciljnih sustava. Vjerojatnost da će doći do cyber napada na autonomna vozila je veća uslijed ranjivosti koje mogu postojati unutar softverske aplikacije koja se koristi za komunikaciju i upravljanje vozilima.

Ključne točke rizika koje nosi napad na računalnu sigurnost sustava:

- Fizička šteta
- Nedostupnost IT sustava I pristupa mrežama
- Gubitak ili brisanje podataka
- Oštećenje ili gubitak podataka, integriteta podataka
- Kršenje podataka koje vodi do ugrožavanja treće strane povjerljivim informacijama, uključujući osobne podatke
- Odavanje poslovnih tajna, istraživanja I razvoja, te druge osjetljive informacije
- Izravni financijski gubitak kao rezultat krađe
- Oštećenje ugleda [4]

[4]ETSI, “Intelligent Transport Systems (ITS)”; Edward Fok, “An Introduction to Cybersecurity issues in Modern Transportation Systems”, ITE Journal, July 2013

Konstantan protok podataka kroz mrežu

Kako prometne mreže postaju pametnije i tehnološki razvijenije, one također postaju i sve više izložene i podložne “cyber” napadima, odnosno napadima hakera. To nije problem koji se može jednostavno zanemariti ili staviti sastrane. Što se prije prijevoznici ozbiljno pozabave računalnom sigurnošću, kad prijeđu u eru pametnog prijevoza, to prije mogu osigurati svoje sustave. Prometne mreže morat će biti stalno povezane, odnosno “online” kako bi se omogućilo nesmetano strujanje podataka kroz više mreža, aplikacija i sustava. Konstantni protok podataka i informacije koje se odnose na trenutno stanje u prometu nose mnoge pogodnosti. Na primjer sinkronizacija rasporeda javnog gradskog prijevoza, informacije o radovima na cestama, zagušenjima u prometu, prometnim nesrećama i drugo.

Međutim, takav sustav ima i negativne strane, operaterova zadaća je upravljanje i nadzor velikog protoka i količine podataka što zahtjeva veliku pozornost. Takav posao može utjecati na pozornost operatera, te prouzročiti da mu promaknu potencijalne ranjivosti, dopuštajući hakerima da pristupe velikoj količini podataka, manevriraju njima te potencijalno napadima ugroze ljudske živote i čine štetu. Da bi se nosili s ovom prijetnjom, operateri će morati biti stalno na oprezu. Podaci pružaju operaterima vidljivost njihove fizičke infrastrukture u stvarnom vremenu, ta se vidljivost odnosi i na digitalne mreže.

Uz prava rješenja za nadzor podataka, operatori mogu mapirati cijelu mrežu, te pronaći potencijalna visoko rizična i ranjiva mjesta, koristiti te podatke za izradu odgovarajućih strategija odgovora na računalne napade, umanjujući rizik od poremećaja i prijetnji. To je stalan proces, ali s vremenom postaje lakši uz korištenje pravih sustava i načina razmišljanja. Osim toga, kako operateri nastavljaju jačati svoju mrežu, mreža će postati sve otpornija na nove prijetnje. Najčešći primjer napada na mrežu su zlonamjerna krađa podataka

2.1 Razvoj i nejasnoće između operativne i računalne sigurnosti

Nažalost, većina operatera upravlja računalnim rizikom kao jedinstvenim slojem, promatrajući ga odvojeno od fizičkog sloja. Usprkos tome što postoji sve veća ovisnost o

sustavima za upravljanje prometom (TMS), za usmjeravanje vozila, upravljanja signalizacijom ili o podacima za optimizaciju prometa na cijeloj ruti.

Kako raste ovisnost između operativne sigurnosti i računalne sigurnosti, operateri će se suočavati sa pritiscima osiguranja sigurnosti putnika i tereta, istovremeno štiteći digitalnu infrastrukturu na kojoj sve više rade. Zbog toga računalnu sigurnost i sigurnost putnika i tereta potrebno je tretirati kao dijelovi iste cjeline. Takav se pristup usredotočuje na spajanje tih elemenata u budućim transportnim sustavima, suprojektiranje i zajedničko testiranje oba aspekta u svim elementima mreže.

Na primjer, operateri mogu pokušati razumjeti opseg kako će njihov rad – bio uspješan ili neuspješan - unutar različitih dijelova sustava utjecati na sigurnost i zaštitu njegove cjeline. To bi dovelo do sustava s zajednički dizajniranim sigurnosnim i zaštitnim mjerama koji se međusobno nadopunjuju ili automatski izoliraju jedan od drugog, u slučaju kršenja.

U naporima da poboljšaju svoju sigurnost, operatori također riskiraju da ih svlada sve veća digitalna složenost. Mogu biti “poplavljeni” rastućom tehničkom složenošću - poput hardverskih sukoba ili različitih sigurnosnih standarda čak iako nastavljaju digitalizirati postojeće rute ili skalirati operacije kako bi zadovoljili sve veću urbanu potražnju. Kao i u bilo kojem drugom poslu, operateri mogu smanjiti ovu neizbježnu razinu složenosti i pritiska udruživanjem s pravim skupom dobavljača i pružatelja usluga.

Uz potporu vladajućih organa, operateri bi trebali usko surađivati s dobavljačima kako bi osigurali učinkovito ispitivanje uvjerenja za opremu, sustave i softver. S rastućom prijetnjom računalnih napada, industrija se neprestano razvija i forsira sve veće razine standardizacije, certificiranja I zajedničkih procesa, posebno neovisne procjene – proizvoda I rješenja dobavlja - ča.

Metode napada za hakiranje autonomnih vozila dijele se na nekoliko klasificiranih kategorija koje uključuju: VANET (engl. Vehicle Adhoc Network) napade, napade na hardware, napade koji iskorištavaju ranjivosti senzora vozila i druge razne napade.

2.2 Napadi na VANET mrežu

VANET mreža (engl. Vehicular Ad Hoc Network) je bežična mreža decentraliziranog tipa koja je nastala od MANET mreže (engl. Mobile Ad Hoc Network). MANET mreža je prva ad-hoc mreža koja je bila u potpunosti razvijena. Obilježja ad-hoc mreža su da nemaju stabilnu infrastrukturu, već svaki čvor unutar same mreže sudjeluje u slanju i primanju podataka. [5]

Ad-hoc mreže mogu biti velikih razmjera što dozvoljava veliki broj korisnika i neograničenu površinu. Brzina samih korisnika, odnosno vozila može biti dosta velika, kao npr. vožnja na autocesti, međutim onda promet ne smije biti pregust, kako bi mreža mogla učinkovito funkcionirati. Što je manja brzina vozila, ad hoc mreža dozvoljava veću gustoću prometa. Što se tiče izvora napajanja, ad hoc mreže nemaju ograničenja. To je jedan od preduvjeta da računalne performanse budu visoke. Za samo kretanje vozila je već poznat uzorak kretanja zbog poznavanja cesta. Osim toga poznate su i veličine čvorova kao visina i širina čvorova. [6]

VANET napadi uključuju napade na unutarnju i vanjsku mrežu, te distribuirane napade uskraćivanja usluge. VANET mreže trenutno najviše istražuje automobilska industrija zbog njihovih mogućnosti poboljšanja učinkovitosti, sigurnosti u prometu i usluga s dodanom vrijednosti. VANET mreže također mogu transformirati pristup u kojem ljudi putuju stvaranjem sigurne, interoperabilne komunikacijske mreže koja uključuje uređaje poput mobitela, prometne signalizacije, autobusa i automobila.

Međutim, VANET mreže su ranjive na značajne cyber-napade koji mogu pokvariti mreže što rezultira gubitkom novca, života i vremena. Jedna od tehnika napada internetskih mreža u VANET-u su napadi na šifru i ključ. Povezana vozila koriste lozinke i ključeve kao sigurnosne mjere. Njih se nastoji probiti kroz nekoliko pokušaja softvera za probijanje lozinki pomoću metode grube sile za oporavak lozinke. Potrebno je obrazložiti da je napad grubom silom uobičajeni pristup koji

[5] Badis, Hakim; Rachedi, Abderrezak - Modeling and Simulation of Computer Networks and Systems. LIGM - Laboratoire d'Informatique Gaspard-Monge, 2015.

[6] Pattnaik O.; Pattanayak B.; - Performance Analysis of MANET and VANET based on Throughput Parameter. Nalanda Institute of Technology, 2017.

hakeri koriste za razbijanje lozinki, uključujući i druge Wi-Fi lozinke koje se koriste za povezivanje vozila i osobnih povezanih uređaja.[7]

Općenito, komunikacijski kanal između vozila i uređaja uspostavlja se putem GSM, Wi-Fi i Bluetooth protokola koji su osjetljivi na napade i sadrže poznate slabosti i ranjivosti koje hakeri mogu ugroziti. Na primjer, povezivanje vozila sa pametnim telefonom izaziva neke rizike jer vozilo komunicira s nepoznatim uređajem. Osim toga, prijenos podataka uslugama u oblaku povećava rizik od ozbiljne prijetnje vozilima, jer bi podatkovni centar mogao biti ugrožen, a vozilo će komunicirati sa sumnjivim poslužiteljem.

Štoviše, mrežni napadi V2V (od vozila do vozila) uključuju promjenu trake, pretjecanje susjednih vozila, razmjenu podataka u vožnji i na raskrižju. Neki napadači također mogu koristiti tehnike lažnog predstavljanja kada se zlonamjerno vozilo lažnim identitetom poveže s glavnim vozilom, a zatim uspostave komunikaciju koja šalje zlonamjerne podatke dok prima kritične informacije, hvata ih, zatim zapisuje i pohranjuje.[8]

Uz to, mogući mrežni napadi V2I (vozila na infrastrukturu) koji bi se mogli pokrenuti izvana uključuju glavno vozilo koje uspostavlja vezu s određenom infrastrukturom, a zatim počinje primati i prenositi informacije. Vozilo je povezano sa čvorovima stanične mreže i inteligentnim prometnim znakovima koje će napadači zlonamjernim softverom vjerojatno iskoristiti, lažno predstavljati ili zaraziti. Ova metoda omogućuje hakerima pristup putem stra-žnjih vrata koji ulazi u upravljačke jedinice motora (ECU) i mrežu vozila.

Napokon, DDoS (Distributed Denial of Service) napadi su najčešći rizici koje većina autonomnih vozila može doživjeti. DDoS napad je napad na računalni servis kojim se korisnicima onemogući njegovo korištenje. Usluge vozila na kraju se uskraćuju korištenjem brojnih tehnika poput zaraze zlonamjernim softverom, koja zauzvrat remeti protok prometa i može prouzročiti

[7] Pattnaik O.; Pattanayak B.; - Performance Analysis of MANET and VANET based on Throughput Parameter. Nalanda Institute of Technology, 2017.

[8] Mohammed Ali Hezam Al Junaid1; Syed A. A; Mohd Nazri Mohd Warip; Ku Nurul Fazira Ku Azir; Nurul Hidayah Romli: Classification of Security Attacks in VANET: A Review of Requirements and Perspectives. School of Computer and Communication Engineering University Malaysia Perlis, Malaysia, 2018.

štetu na okolnoj infrastrukturi. Ove tehnike napada mogu dovesti do sudara vozila koji prijete životima putnika.

2.3 Napadi na hardware računala

Hardverski napadi uključuju sljedeće kategorije: nevaljala ažuriranja, napad zasnovan na OBD portu i napadi na ECU ugrađeni software (engl. Firmware).

2.3.1 Napadi na OBD port

Ugrađena dijagnostika (OBD) je pojam koji se koristi kod automobila te poziva na sposobnost samodijagnostike i izvještavanja vozila. OBD sustavi omogućuju vlasniku vozila ili serviseru pristup statusu različitih podsustava vozila, te su OBD priključci prisutni u gotovo svim vozilima proizvedenim od 2008. To je ručni uređaj poput USB-a koji mora biti povezan s vozilom kroz priključak koji je općenito prisutan ispod ploče s instrumentima nasuprot suvozačkom sjedalu, koji se zatim povezuje s računalom putem žičane veze putem USB priključka ili putem bežične veze putem Bluetootha. Jednom spojeno računalo može slati i primati podatke u i iz ECU-a vozila, a eventualno iskorištavanje može također manipulirati paketima podataka i ubrizgati zlonamjerne pakete u mrežu vozila. [9]

Hakeri mogu pokretati napade na OBD priključak izvršavajući logičko i fizičko ažuriranje ugradbenih softvera. Međutim, ovu prijetnju lako je ublažiti korištenjem asimetrične kriptografske arhitekture (javno-privatni ključ) koja potvrđuje da se ažuriranja firmvera preuzimaju iz legitimnog izvora. Posljednji zabilježeni napad ove prirode odnosio se na BMW-ova vozila koja su imala potencijal za reprogramiranje putem OBD priključka. Napadi zasnovani na OBD portu klasificirani su kao niskotarifni incidenti kojima haker treba priključiti uređaj u OBD

[9] Amara Dinesh Kumar; Koti Naga Renu Chebrolu; Vinayakumar R; Soman KP: A Brief Survey on Autonomous Vehicle Possible Attacks,Exploits and Vulnerabilities. U: eprint arXiv:1810.04144, Listopad 2018.

priključak kako bi omogućio zaobilaženje sustava za imobilizaciju vozila i programirao novi ključ. [10]

Slika 1. Prikazuje OBD skener u radu [11]

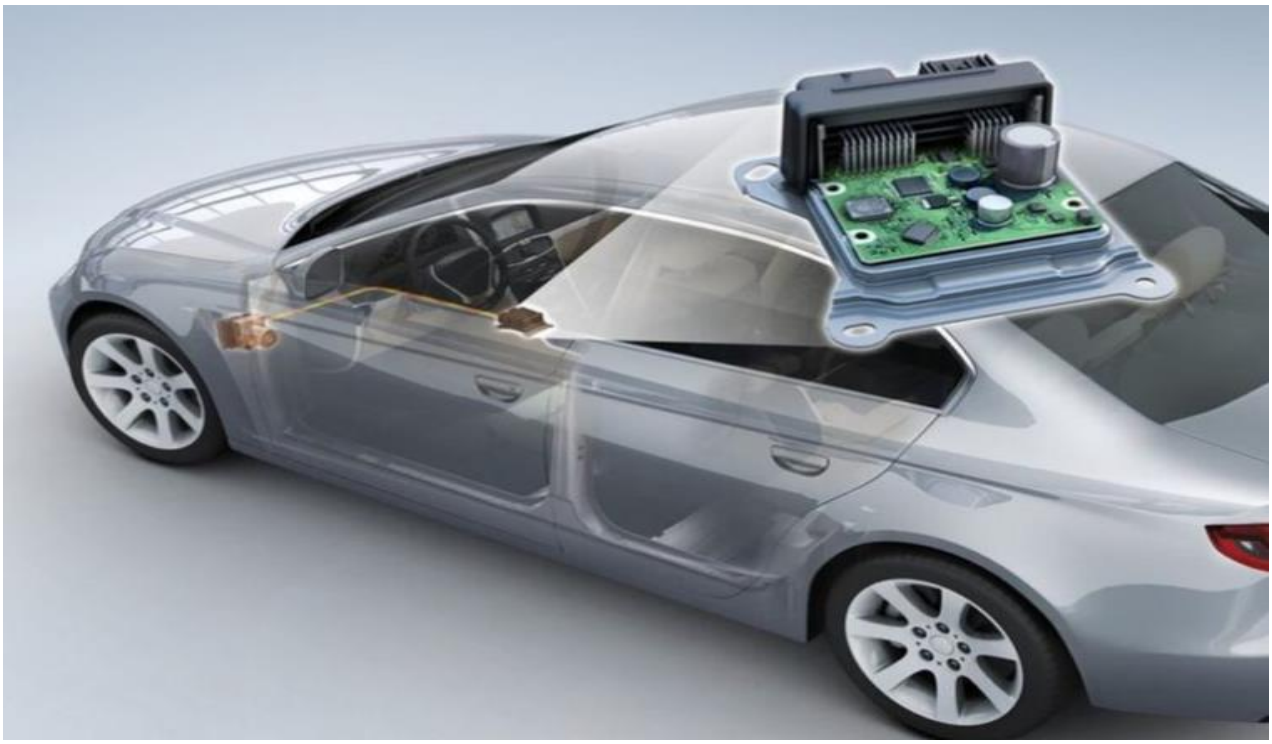
OBD priključak komunicira s ECU-ima i preko sabirnice CAN (engl.Control Area Network). CAN sabirnica mreža koje se na vozilo povezuju putem OBD priključka ispod vozačeve nadzorne

[10] Dan Klinedinst; Christopher King : On Board Diagnostics: Risks and Vulnerabilities of the Connected Vehicle
[11] https://www.quotidianomotori.com/automobili/migliori-obd2-scanner-diagnostici/

ploče, pomoću dongle- a ili adaptera za sučelje. Uređaji se mogu povezati s računalom putem USB priključka u ožičenom okruženju ili bežično pomoću Bluetooth tehnologije. Nakon povezivanja s računalom, uređaj ima mogućnost slanja i primanja podataka na i s ECU-a. Tijekom prijenosa, komunikaciju mogu presresti hakeri i manipulirati paketima podataka koristeći zlonamjerne pakete koji se šalju u mrežu vozila. Glavni problemi koji olakšavaju uspješno hakiranje OBD dongle-a su izloženi ključevi, slaba enkripcija i otmica u komunikaciji.

2.3.2 Napadi na ECU ugradbene softvere

ECU (upravljačka jedinica motora) elektronički je upravljački modul za senzore i aktuatore bilo kojeg podsustava u vozilu, a tipično vozilo sastoji se od više od 100 ECU-a . Kod ECU koristimo kôd kako bi podsustavi bili sigurni i osigurani, no nedavni napadi ukazali su na to da se ECU kodovi mogu iskoristiti ponovnim bljeskanjem ECU-a i izmjenom firmware- a koji je prilagođen određenim vozilima i uvođenjem nenamjernih i zlonamjernih aktivnosti.



Slika 2. Izgled ECU- a i mjesto gdje se upravljačka jedinica motora nalazi u vozilu [12]

[12] http://www.marketstatsnews.com/automotive-electronic-control-unit-market/

Ova tehnika hakiranja poznata je kao napad izravnog pristupa, nazvan tako od strane stručnjaka iz auto- industrije. Haker ažurira ugrađeni softver ECU-a korištenjem vanjskog sučelja koje im omogućuje izmjenu funkcionalnosti ECU-a. Manevrirajući memorijom ECU-a i neovlaštenim promjenama sigurnosnih ključeva te održavanjem integriteta programskog koda ECU-a i njegovih ažuriranja pomoću tehnika raspršivanja i provjere autentičnosti za ažuriranje softvera. [13]

2.3.4 Neispravna ažuriranja

Neispravna ažuriranja uzrokovana su ažuriranjima firmware-a povezanih vozila koja nisu ispravno provedena. Prvenstveno, većina ovih ažuriranja ne proizlaze od strane stvarnih proizvođača, a ponekad im nedostaju odgovarajuća ažuriranja sa sigurnošću i zaštitom. To stvara ranjivosti u vozilima koja mogu dovesti do "curenja" privatnih podataka. Ažuriranja omogućuju napadačima da generiraju veću ranjivost unutar firmware-a vozila putem zlonamjernog softvera, stječući kontrolu nad firmware-om povezanih vozila. Iskorištavanje ovog pristupa hakeri provode na dva načina koji uključuju daljinski i fizički pristup. [14]

U kontekstu fizičkog pristupa, ECU je integriran s fizičkim slojevima, povećavajući šanse za mrežne napade. Hakeri mogu izravno iskorištavati komunikacijske module, kontrolu i podatke senzora. Mrežni napadi se mogu pokrenuti na elektroničke module automobila izravnim napadom koji uzrokuje učinak preopterećenja na fizičkim slojevima. S druge strane, iskorištavanje daljinskog pristupa provedeno je putem veza autonomnog vozila na Bluetooth, Wi-Fi, 4G i druga bežična sredstva. Veza na internet koji koristi ovu metodu predstavlja značajan rizik. Presudno je da čak ni proizvođači automobila nisu sigurni u potrebne radnje koje bi trebalo poduzeti u

[13] M. H. Eiza; Q. Ni; - Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity. U: IEEE Vehicular Technology Magazine, 6/2017. Str. 45-51

[14] Mo, Y.;Garone, E.;Casavola, A.; Sinopoli, B.: "False data injection attacks against state estimation in wireless sensor networks". Decision and Control (CDC), 2010 49th IEEE Conference. Siječanj 2011.

ublažavanju ili čak oporavku od izazova uzrokovane napadom. U ovakvim slučajevima hakeri imaju prednosti upravljanja autonomnim vozilima.

2.4 Napadi na senzore vozila

Senzori u vozilu integrirani su s različitim tehnologijama koje su ranjive, uključujući globalni sustav pozicioniranja (GPS), inercijalnu mjernu jedinicu (IMU), detektor svjetla i dometa (LiDAR) te monoskopske i stereoskopske kamere.

GPS tehnologija koristi se za određivanje mjesta svakog vozila i navigaciju kroz područja putovanja. Operateri i kontrolori vozila moraju koristiti GPS podatke za lociranje i navigaciju vozila. Broj satelita povećan je u javnoj domeni kako bi se operaterima omogućio lak pristup GPS podacima jer je to bio izazov u prethodnim procesima lociranja i navigacije. Međutim, pružanje i mogućnost besplatnog pristupa GPS podacima s jasnom arhitekturom pomaže napadačima da manipuliraju podacima i zavaraju operatere davanjem pogrešnog smjera ili ponekad kontroliraju usmjeravanje vozila. Otvorena tehnologija poput GPS-a izaziva zabrinutost u vezi sa sigurnošću i zaštitom putnika. Napadači se koriste tehnikama poput ometanja i GPS prijevara prenošenjem nerealnih podataka ili signala kojima je cilj poremetiti ili obmanuti signale. GPS uređaji dizajnirani su da koriste jače signale pod pretpostavkom da su informacije učinkovitije. Prijemnici koji koriste ovaj algoritam mogu favorizirati jači, lažni signal podataka koji može dovesti do toga da operativni sustav promijeni položaj vozila. Trenutno je postupak izvođenja uspješnih GPS napada medijski pokriven, uključujući znanstvene članke i dostupan u javnoj domeni.[15]

Inercijalna mjerna jedinica uključuje kombinaciju akcelerometara i žiroskopa koji nude podatke za orijentaciju, ubrzanje i brzinu vozila. Te se varijable također koriste u praćenju promjena u dinamici okoliša kao što je gradijent karte. Hakeri mogu iskoristiti te sustave mijenjanjem podataka koje pružaju senzori tako da IMU ne prepozna gradijent karte ili ceste. Pogrešne informacije uzrokuju da se vozila sporije kreću nagibnim cestama, a zauzvrat usporavaju

[15] S. Parkinson; P. Ward; K. Wilson; J. Miller; - ”Cyber threats facing autonomous and connected vehicles: Future challenges”. U: IEEE Transactions on Intelligent Transportation Systems, 11/2017. Str. 2898 - 2915

ubrzanje autonomnog vozila. Senzori nagiba i žiroskopi koriste se u određivanju nagiba ceste i održavanju sigurnog rada.

Senzor detekcije i dometa svjetlosti (LiDAR) je još jedan senzor koji može postati meta napada koji hakeri koriste u iskorištavanju ranjivosti autonomnih vozila i mreža. LiDAR se koristi u izbjegavanju, otkrivanju objekata i lokalizaciji okoliša. Rad LiDAR-a temelji se na tehnologiji vremena potrebnog za putovanje svjetlosti do i od objekta, čime se određuje udaljenost između vozila i predmeta. Hakeri mogu iskoristiti rad ove tehnologije slanjem zlonamjernih signala na istoj frekvenciji skenerima čineći da vozilo pretpostavlja da je otkriven objekt. Vjerojatno će se vozilo zaustaviti ili kretati sporije, što negativno utječe na stvarno planiranje i programiranje vozila.[16]

Napokon, senzori monoskopskih i stereoskopskih kamera također su ugroženi od strane hakera, jer se koriste u autonomnim vozilima za otkrivanje prometnih znakova, traka, zapreka i prednjih svjetala. Hakeri mogu djelomično onemogućiti funkcioniranje kamera upotrebom gornjih svjetala obližnjeg vozila. Ovim napadom vozilo otkriva lažne podatke kao što su predmeti i farovi. Napadi koji koriste ovu metodu utječu na standardnu funkcionalnost vozila, posebno u izvršavanju uloge otkrivanja različitih predmeta poput trake i prepreka. Uz to, još jedna moguća tehnika napada koja cilja kamere je automatska ekspozicija, gdje uvođenje dodatnog svjetla smanjuje ekspoziciju i osjetljivost. Dodatno svjetlo, u ovom slučaju, mogu se pojaviti iz farova drugih vozila ili gorionika. Ovaj napad skriva ključne informacije vitalne za vozilo na cestama kao što su pješaci, rubovi cesta i prometni znakovi.

2.5 Ostali napadi na autonomna vozila

Razni napadi uključuju sve ostale taktike, postupke i tehnike hakiranja koji se mogu koristiti za iskorištavanje različitih ranjivosti i funkcionalnosti autonomnih vozila. Primjeri tih napada uključuju infekcije zlonamjernim virusom i prijetnje aplikacijama za mobilne mobitele.

[16] Jamal Raiyn: "Data and Cyber Security in Autonomous Vehicle Networks ". U: December 2018, Transport and Telecommunication Journal, 12/2018.

Hakeri koriste zlonamjerni softver, metoda napada na autonomna vozila za iskorištavanje ranjivosti paketa za ažuriranje softvera, dizajna i implementacije komponenata i mrežnih podsustava u vozilu, kao i ranjivosti operativnog sustava koji se koristi u vozilu. Infekcija zlonamjernim softverom može kontinuirano uzrokovati ozbiljnu eksploataciju cijelog sustava i podsustava. Na primjer, infekcija zlonamjernim softverom može se koristiti za uništavanje funkcionalnosti nekih značajki autonomnog vozila, uključujući zaključavanje radija automobila tako da ga korisnici ne mogu uključiti. Mnoge vrste zlonamjernog softvera ili virusa instalirane na daljinu mogu vozaču ometati proizvoljno uključivanje i isključivanje radija ili neočekivano povećanje glasnoće ili onemogućavanje sigurnosti ključnih komponenti vozila kao što su vrata i otvarati ih bez djelovanja putnika. [17]

Drugi scenariji koji napadači mogu koristiti su zlonamjerni softver za slanje izmijenjenih sigurnosnih podataka osmišljenih kako bi kod putnika izazvao sumnju i strah. Iako je poznato da većina autonomnih vozila radi na Linux operativnom sustavu za koji je utvrđeno da je otporan na napade, nedavna istraživanja pokazuju da je napad malware-a na OS zasnovan na Linuxu u porastu. Napadi ove prirode čine autonomna vozila skupinom visokog rizika od napada zlonamjernog softvera. Štoviše, zlonamjerni softver ili zlonamjerni kôd mogu zaraziti kontrolne centre što rezultira kolapsom sustava. [18]

Prijetnja automobilskoj industriji preko mobilnih uređaja još je jedna tehnika napada koju bi proizvođači i istraživači industrije trebali razmotriti. Mobilni uređaji i aplikacije poput androidovih automobilskih sučelja ranjivi su na napade, a njihova povezanost s autonomnim vozilima povećava šanse da vozila budu meta.

[17] J. A. P. Marpaung; M. Sain; H. J. Lee;: "Survey on malware evasion techniques: State of the art and challenges,". Proc. Int. Conf. Adv.Commun. Technol., PyeongChang, Korea, 2012

[18] Maurer, Markus, J. Christian Gerdes; Barbara Lenz; Hermann Winner;: "Autonomous Driving: Technical, Legal and Social Aspects". 1st ed. 2016

Opasnosti, prijetnje i problemi u razvoju vozila

Prijetnje u autonomnim vozilima različite su vrste kibernetske sigurnosti koje će vjerojatno iskoristiti višestruke ranjivosti mreža, infrastrukture i funkcionalnosti vozila. Autonomna vozila nailaze na višestruke prijetnje, uključujući sljedeće eksploatacije i rizike.

Napadači mogu uvesti sljedeće prijetnje autonomnim vozila:

- ugasiti vozilo
- daljinski preuzeti i kontrolirati vozilo
- špijunirati putnike u vozilu
- otključati vozilo uzrokujući poremećaje u prometu
- pratiti vozilo
- instalirati zlonamjerni softver u vozilo
- onemogućiti sigurnosne sustave i ukrasti vozilo ili vozni park

Budući da vozila koriste softvere za svoj kontrolni mehanizam i komunikaciju, kao i pohranu podataka, hakeri ih mogu daljinski iskoristiti korištenjem određenog zlonamjernog softvera, poput **Ransomwarea**. Ransomware je posebna vrsta zlonamjernog softvera koji iznuđuje novčanu otkupninu od svojih žrtava tako što im zaprijeti da će objaviti, obrisati ili zabraniti pristup važnim osobnim podacima. Kad bi hakeri mogli daljinski eksploatirati računala i preuzeti kontrolu nad njima u potpunosti, došlo bi do opasnosti od otmice vozila, te traženja naknada za povrat istih. Industrijski programeri i istraživači upozoravaju na moguće napade koji mogu u potpunosti kontrolirati funkcionalnost i infrastrukturu vozila, isključujući ga i čineći ga beskorisnim. Uz to, napadači mogu staviti ECU ili TPMS (prijemnik senzora tlaka u gumama) u nepopravljivo stanje ili se vozilo može ugasiti kao posljedica aktivacije sigurnosne značajke.

Špijuniranje je moguće napadom na bežične komunikacije između pametnih telefona vlasnika i mreže vozila. Napadači mogu prisluškivati razmijenjene informacije i vraćati lažne podatke natrag kritičnim senzorima vozila. Napadači se također mogu koristiti alatima kao što je **Vehicle Spy** koji je dizajnirao funkcionalnosti promjene komunikacijskih protokola vozila i obrnuo CAN. Hakeri bi mogli koristiti alat za otkrivanje ranjivosti u vozilu paralelno s drugim metodama

kao što su skriptiranje na njuškalici, bljeskanje ECU-a, kalibracija memorije ili napredne značajke Node Simulation. Hakeri koriste dijagnostičke alate ili testove koji šalju zahtjeve sustavima za obavljanje određenih zadataka, a zauzvrat generiraju signale poput CAN paketa. Signali se mogu presresti i koristiti za modificiranje firmwera vozila. Na primjer, dijagnostički alati ponekad mogu zatražiti otključavanje vrata automobila. Ta će pojava ili prijetnja vjerojatno prouzročiti ozbiljne nesreće, poremetiti promet i druge višestruke posljedice.

Ugrožavanje sigurnosti vozila značajan je rizik za putnike i opću sigurnost na cesti. Zlonamjerni softver može biti instaliran na konzoli za informiranje i zabavu, dobivajući prilike za pristup internoj mreži sabirnice CAN i uvid u podatke koje korisnici prikazuju, kao što je mjesto vozila.

3. Autonomna vozila

Autonomno vozilo ili vozilo bez vozača je vozilo koje može samostalno upravljati i obavljati potrebne funkcije bez ikakve ljudske intervencije, kroz sposobnost da osjeti svoju okolinu. Autonomno vozilo koristi potpuno automatizirani sustav vožnje kako bi vozilo moglo reagirati na vanjske uvjete kojima bi upravljao ljudski vozač. Autonomna vozila istovremeno koriste razne senzore za prepoznavanje okoline, kao što su radari, lidari, sonari, GPS, odometrija i jedinice za inercijsko mjerenje.

Slika 3. Autonomno vozilo tvrtke Ford i Argo AI [19]

Prvi automobil je razvijen još u industrijsko doba 19. stoljeća, kada je njegov razvoj obilježila metalna industrija. Danas su motorna vozila tehnički usavršena, lijepo dizajnirana, obilježena informacijskom tehnologijom te rješenjima za sigurniju i ekološki prihvatljivu vožnju,

[19] https://spectrum.ieee.org/ford-signs-up-to-use-nasas-quantum-computers

a budući automobili će biti „pametni automobili“ koji će za autonomnu vožnju koristiti umjetnu inteligenciju.

3.1 Ključne komponente I principi rada autonomnih vozila

Autonomna vozila koriste razne senzore i komponente kako bi uspjesno opažala i percepirala svoju okolinu i ono što se oko njih događa, te pomoću tih informacija uspješno manevrirala cestama. Komponente autonomnih vozila uključuju razne senzore poput radara, lidara, sonara, GPS-a, odometrije i inercijalnih mjernih jedinica. Također, koriste se složeni algoritmi, sustavi strojnog učenja i moćni procesori, sve sa ciljem stvaranja što uspješnijeg i sigurnijeg vozila, samim time i prometa. Napredni upravljački sustavi tumače informacije dobivene od senzora kako bi identificirali odgovarajuće navigacijske putove, kao i prepreke i relevantne signalizacije. Tehnologija se primjenjuje za osobna vozila, takozvane “robotaksije”, povezane vodove, odnosno kolone vozila, te kamione.

Razine autonomne vožnje

Postoji šest različitih stupnjeva automatizacije i kako se razine povećavaju, povećava se neovisnost automobila bez vozača u pogledu upravljanja radom.

- **RAZINA 0**, automobil nema kontrolu nad svojim radom i ljudski vozač obavlja svu vožnju
- **RAZINA 1**, ADAS (napredni sustav pomoći vozaču) vozila može podržati vozača bilo upravljanjem, bilo ubrzavanjem ili kočenjem
- **RAZINA 2**, ADAS može nadgledati upravljanje, ubrzanje i kočenje u nekim uvjetima, iako je ljudski vozač dužan i dalje tijekom cijele vožnje obraćati potpunu pažnju na vozačko okruženje, istovremeno izvršavajući i preostale zadatke
- **RAZINA 3**, ADS (napredni sustav vožnje) može izvesti sve dijelove vožnje u nekim uvjetima, ali ljudski vozač mora biti u mogućnosti povratiti kontrolu kada to zatraži ADS. U ostalim uvjetima ljudski vozač izvršava potrebne zadatke
- **RAZINA 4**, ADS vozila može samostalno obavljati sve vozačke zadatke u određenim uvjetima u kojima nije potrebna ljudska pažnja

- **RAZINA 5** uključuje potpunu automatizaciju pomoću koje je ADS vozilo u stanju izvršavati sve zadatke u svim uvjetima i od ljudskog vozača nije potrebna pomoć u vožnji. Potpuna automatizacija bit će omogućena primjenom 5G tehnologije koja će omogućiti vozilima da komuniciraju ne samo jedni s drugima, već i sa semaforima, znakovima, pa čak i samim cestama [20]

Kako klasični tako i autonomni automobili moraju biti privlačni svojim korisnicima, nezavisno od toga da li ga posjeduju ili ne. Ako služi kao dio zajedničke usluge ili individualno, automobili budućnosti ostvariti će svoju potražnju na tržištu zahvaljujući i svom dizajnu. Oblik automobila i njegovih dijelova proizlazi iz njihove funkcije. Prema viziji studije Autonnomous Driving, dizajn autonomnih vozila temelji se na tri oblika automobila: mini - za uporabu na kraće udaljenosti, midium - za srednje udaljenosti i personalizirana vozila

Mini vozila primarno će se koristiti u gradovima i prigradskim naseljima. Takva vozila pružaju veliku okretljivost, domet 15-20 km, kapacitet 1-2 putnika. To su vozila za rentanje (dijeljenje), visoko pouzdana i nisu skupa za nabavu i održavanje.

Midium vozila će se također primarno koristiti u gradovima i prigradskim naseljima. Takva vozila pružaju veći komfor, nude više prostora za prijevoz 4+ putnika. To su također vozila za rentanje. Personalizirana vozila, bilo za fizičke ili pravne osobe, nemaju ograničenja, ni po dometu, ni komforu, ni obliku (limuzina, hatchback, crossover, SUV). Obzirom na to da se vozač ne fokusira na upravljanje vozilom, dizajn interijera i medijsko-zabavna industrija preispitat će što rade putnici autonomnih vozila kada su na putu. U praksi će se pokazati da li putnici imaju više vremena za posao i / ili slobodno vrijeme. U oba slučaja, vizualna poruka vanjskog i unutarnjeg uređenja stoga mora biti inteligentno osmišljena, stvarajući automobil kao tržišni proizvod.[21]

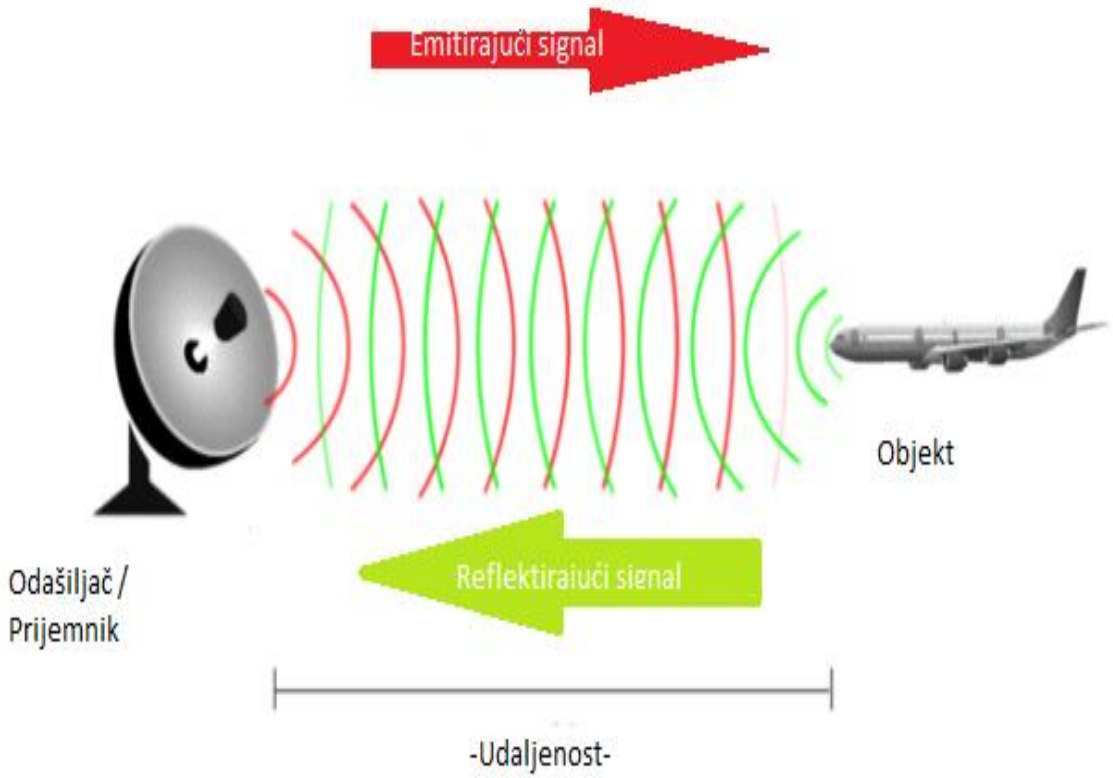
Autonomni automobili stvaraju i održavaju mapu svoje okoline na temelju različitih senzora smještenih u različitim dijelovima vozila. Tri primarna autonomna senzora za vozila su

[20] Bosnjak, I.; Inteligentni transportni sustavi 1. Sveučilište u Zagrebu, Fakultet prometnih znanosti, Zagreb, 2006.
[21] Study by Autonomous Driving, Think ACT, Ronald Berger Strategy Consultatnts Gmbh, Munchen, 2014.

kamera, **radar** i **lidar**. Radeći zajedno, pružaju automobilima vizualne prikaze okoline i pomažu mu u otkrivanju brzine i udaljenosti obližnjih predmeta, kao i njihovog trodimenzionalnog oblika.

3.2 Radar

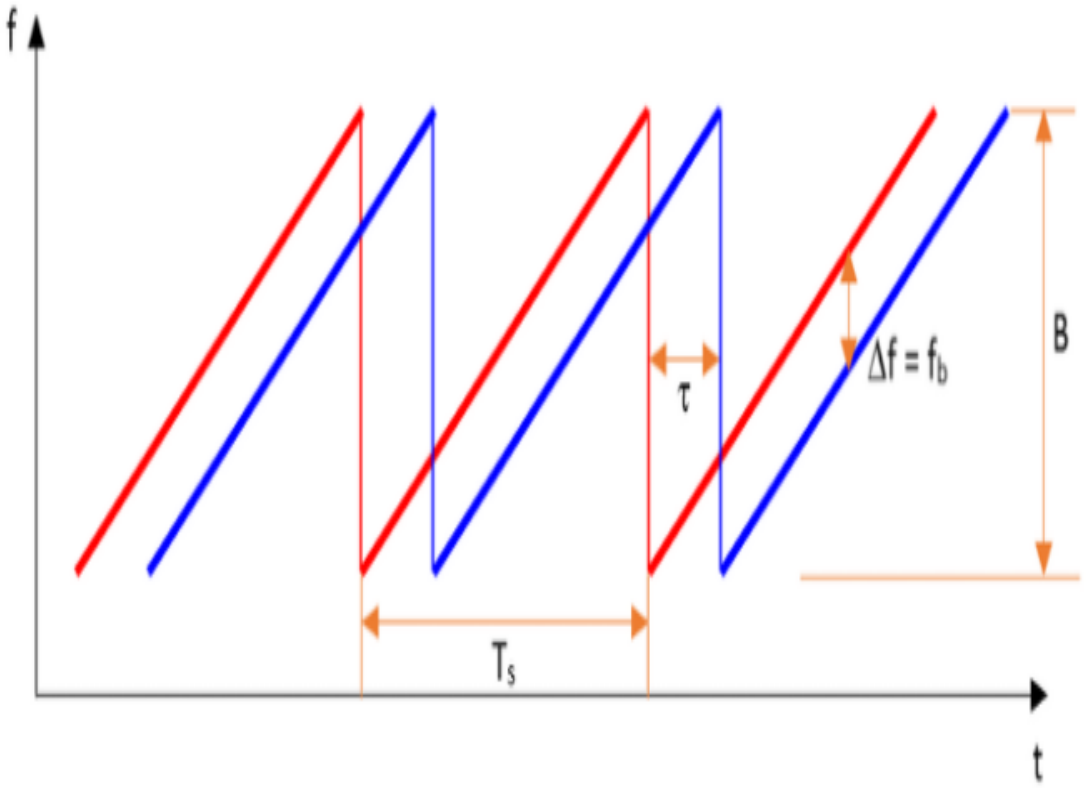
Radar je senzor koji se koristi još od 30-ih godina 20. stoljeća. Izvorno korišten od strane vojske za otkrivanje neprijateljskih zrakoplova, postao je neizostavna komponenta u arsenalu svake vojske. Danas je to tehnologija koja se koristi u vozilima za prilagodljiv tempomat, te za otkrivanje prepreka I objekata koja se nalaze u okolini autonomnog vozila.



Slika 4. Princip rada senzora RADAR- a

RADAR je skraćenica od Radio Detection And Range (otkrivanje i određivanje udaljenost radio valovima). Djeluje emitirajući elektromagnetske (EM) valove koji se reflektiraju kad naiđu na prepreku. Budući da radi pomoću EM valova, može raditi pod bilo kojim uvjetima.

Postoji mnogo različitih vrsta RADARA, jedan od najpopularnijih i najrelevantnijih u našem slučaju zove se FMCW - Frekvencijski modulirani kontinuirani val. Ova vrsta RADARA zrači kontinuiranom snagom. Može otkriti prepreke na vrlo malim dometima i istodobno može izmjeriti domet i brzinu objekta. Val izgleda ovako: to je signal koji se naziva pilast čija se frekvencija s vremenom može povećavati ili smanjivati.



Slika 5. Pilasti signal FMCW RADAR-a

Hardver FMCW RADARA sastoji se od mnogih stvari:

- Frekvencijski sintetizator - Postavlja val na pravu frekvenciju.
- Pojačalo snage - Pojačava signal kako bi RADAR-i mogli vidjeti na velikim udaljenostima (300 m).
- Antena - Pretvara električnu energiju u elektromagnetske valove koji se šalju u određenom smjeru i reflektiraju (natrag na antenu).

- Frekvencijsko miješalo- nešto što pomaže kod pomicanja frekvencije.
- Procesor - Baš kao i na bilo kojem računalu, procesor pomaže u proračunima, a možemo čak i obraditi signal za strojno učenje, grupiranje, praćenje

Kada emitirani val dosegne objekt, on se reflektira, te se ne reflektira svaki put točno k anteni RADAR-a. U takvim slučajevima koristi se indeks refleksije zvan Radarski presjek (engl. Radar Cross Section), skraćeno RCS, koji uzima u obzir geometriju objekta, smjer u odnosu na RADAR, frekvenciju i materijal objekta.

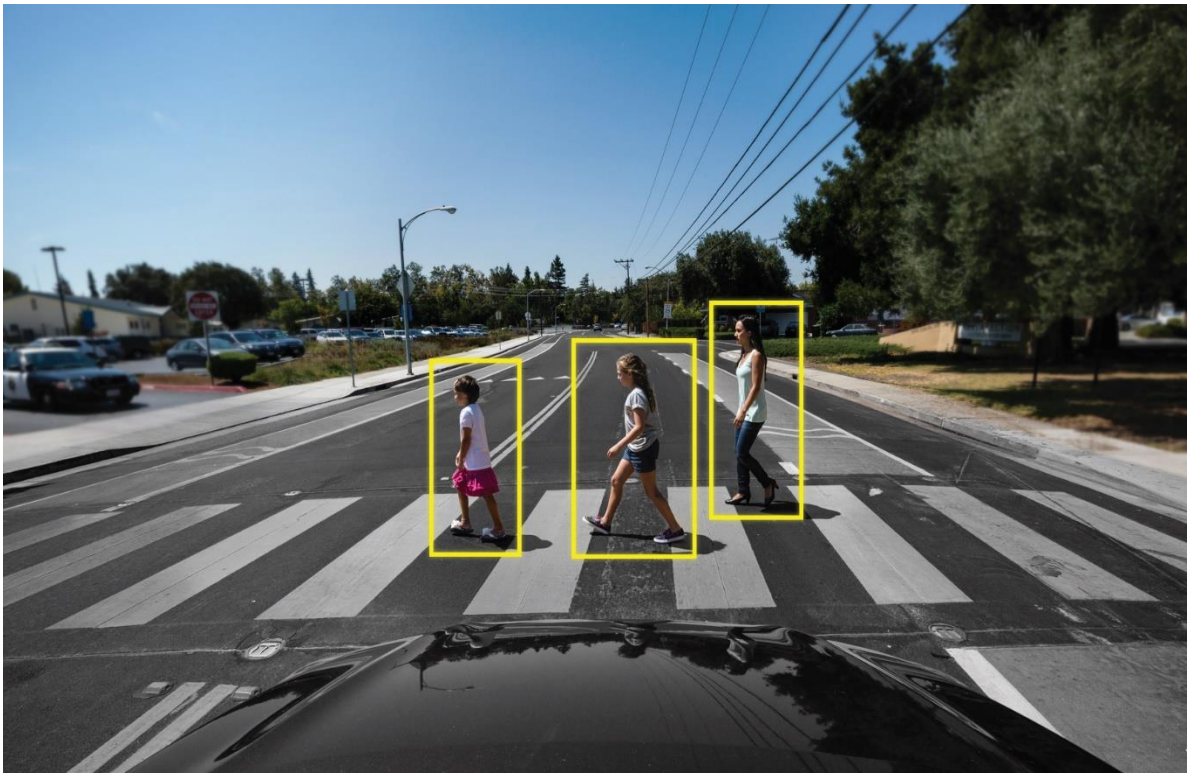
Tehnologija autonomnih vozila može pružiti određene prednosti u usporedbi s vozilima kojima upravljaju ljudima. Jedna takva potencijalna prednost je što mogu pružiti veću sigurnost na cesti - sudari vozila uzrokuju mnogo smrtnih slučajeva svake godine, a automatizirana vozila mogu potencijalno smanjiti broj žrtava, jer će softver koji se koristi u njima napraviti manje pogrešaka u odnosu na ljude. Smanjenje broja nesreća moglo bi umanjiti i zagušenje u prometu, što je dodatna potencijalna prednost koju predstavljaju autonomna vozila. Autonomna vožnja to može postići i uklanjanjem ljudskog ponašanja koje uzrokuje blokade na cesti, posebno u prometu prilikom zaustavljanja i kretanja.

Još jedna moguća prednost automatizirane vožnje je da bi ljudi koji nisu u stanju vožnje - zbog faktora poput starosti ili invaliditeta mogli koristiti automatizirane automobile kao prikladnije prometne sustave. Dodatne prednosti koje dolazi s autonomnim automobilom su uklanjanje umora u vožnji i mogućnost spavanja tijekom noćnih putovanja.

3.3 Video kamere

Od fotografija do videa, kamere su najtočniji način za stvaranje vizualnog prikaza svijeta, posebno kada je riječ o autonomnim automobilima. Video slike pružaju većinu detalja za ljudskog vozača, ali su također prikladne i kao ulazni parametar za visoko automatiziranu vožnju. Autonomna vozila oslanjaju se na kamere postavljene sa svake strane - sprijeda, straga, slijeva i zdesna - kako bi imale pogled od 360 stupnjeva na svoju okolinu. Neki imaju široko vidno polje - čak 120 stupnjeva - i kraći domet. Drugi se usredotočuju na uski pogled kako bi

pružili vizuale velikog dometa. Neki automobili čak integriraju i kamere sa širokokutnim lećama koje pružaju panoramski pogled, dajući cjelovitu sliku onoga što stoji iza vozila da bi se vozilo moglo parkirati. Danas su dvodimenzionalne kamere široko dostupne za prikaz slika, a ponekad na zaslonu postavljaju dodatne informacije, poput kuta volana. Proizvođači automobila luksuzne klase počinju instalirati kamere s virtualnim, trodimenzionalnim prikazima slika.



Slika 6. Prikaz identificiranja objekata ispred vozila pomoću kamere [22]

Da bi trodimenzionalna slika bila realistična, obično su potrebni ulazni signali od šest i više kamera, a potrebno je obratiti posebnu pozornost na usklađivanje, odnosno preklapanje slika kako bi se izbjegao gubitak podataka o slici ili generiranje slika duhova. I za 2-D i 3-D kamere potrebni su senzori slike s vrlo visokim dinamičkim rasponom većim od 130 dB. Ovaj visoki dinamički raspon apsolutno je neophodan za postizanje jasne slike čak i kad izravna sunčeva svjetlost sja u leću. Najbolji dostupni senzori slike na tržištu imaju dinamički raspon od 145 dB s

[22] https://blogs.nvidia.com/blog/2019/04/15/how-does-a-self-driving-car-see/

24-bitnim dubokim sučeljem za ISP (procesor slikovnih signala). Ovaj dinamički raspon znatno je iznad onoga što uobičajeni sustavi leća mogu ponuditi. Druga važna značajka kvalitete je intenzitet svjetlosti senzora slike. Trenutno najbolji dostupan na tržištu ima senzor slike Odnos signala i šuma (SNR) = 1 za osvjetljenje od 1 mlx (Millilux) i brzinu kadrova od 30 sličica u sekundi.

Središnja upravljačka jedinica obrađuje sirove podatke od najmanje šest kamera. Budući da se obrada vrši u softveru, procesor se suočava sa teškim zahtjevima. Dodatni FPGA-i potrebni su za specifično hardversko ubrzanje koje u takvom sustavu uzrokuje gubitak velike snage. Moderne metode kompresije podataka također zahtijevaju velike kapacitete za pohranu.

Kamere postavljene sprijeda su sustavi za srednje i velike domete, “dohvaćaju” područja između 100 i 275 metara. Te kamere koriste algoritme za automatsko otkrivanje objekata, klasificiranje i određivanje udaljenosti od njih. Na primjer, kamere mogu prepoznati pješake i bicikliste, motorna vozila, bočne trake, nosače mostova i rubove cesta. Algoritmi se također koriste za otkrivanje prometnih znakova i signala. Kamere srednjeg dometa u osnovi upozoravaju vozača na poprečni promet, pješake, kočenje u nuždi u automobilu ispred, kao i na otkrivanje traka i signalnog svjetla. Kamere velikog dometa koriste se za prepoznavanje prometnih znakova, kontrolu udaljenosti na temelju video zapisa i vođenje cestom. Za ove sustave fotoaparata nije navedena reprodukcija signala precizna u boji, jer se koriste samo izravni sirovi podaci senzora slike. U pravilu se koristi filtar u boji s RCCC (engl. Red Clear Clear Clear) matricom, koji pruža veći intenzitet svjetlosti od RGB filtra (crveno zeleno plavo) koji se koristi u većini slikovnih kamera. "Red Clear Clear Clear" označava piksel s filterom crvene boje i tri s filtrom neutralne (bistre) boje. Glavna razlika između kamera za srednji i visoki domet je kut otvora objektiva ili FoV, vidno polje. Za sustave srednjeg dometa koristi se vodoravni FoV od 70 ° do 120 °, dok kamere sa širokim rasponom otvora koriste vodoravne kutove od približno 35 °. Budući će sustavi pokušati pokriti srednji i visoki domet isključivo optičkim sustavom. Da bi to uspjelo, slikovni senzori u budućnosti vjerojatno će imati više od 7 milijuna piksela.

Iako pružaju točne vizualne prikaze, kamere imaju svoja ograničenja. Mogu razlikovati detalje okoline, međutim, treba izračunati udaljenosti tih predmeta da bi se točno znalo gdje se

nalaze. Također je senzorima temeljenim na fotoaparatima teže otkriti objekte u uvjetima slabe vidljivosti, poput magle, kiše ili noći.

Slika 7. Detekcija objekata u otežanim uvjetima: samo pomoću kamere, samo pomoću Lidara, pomoću oba senzora [23]

3.3 LIDAR

Lidar (akronim od engl. Light Detection and Ranging: svjetlosno zamjećivanje i klasifikacija) je optički mjerni instrument koji odašilje laserske zrake koje se odbijaju od vrlo sitnih čestica raspršenih u Zemljinoj atmosferi (aerosola, oblačnih kapljica i drugo) i potom registriraju u optičkom prijamniku. LIDAR djeluje kao oko samovozećih vozila pružajući im pogled od 360 stupnjeva. Kontinuirano rotirajući LiDAR sustav šalje tisuće laserskih impulsa svake sekunde. Ti se impulsi sudaraju s okolnim objektima i reflektiraju natrag. Rezultirajuće refleksije svjetlosti zatim

[23] https://www.flir.eu/discover/rd-science/can-thermal-imaging-see-through-fog-and-rain/

se koriste za stvaranje 3D oblaka točaka. Računalo bilježi svaku refleksijsku točku lasera i prevodi ovaj oblak točaka koji se brzo ažurira u animirani 3D prikaz.

Početkom 21.stoljeća LIDAR se prvi put koristi na automobilima, gdje ga je Stanley (a kasnije i Junior) proslavio u Grand DARPA Challengeu 2005. Godine. Stanley, pobjednik Grand DARPA Challengea 2005. godine, upotrijebio je 5 SICK LIDAR senzora postavljenih na krov, uz vojni GPS, žiroskope, akcelerometre i kameru usmjerenu prema naprijed koja gleda iznad 80 m. Sve to pokretalo je šest 1,6 GHz Pentium Linux računala koja su sjedila u prtljažniku.

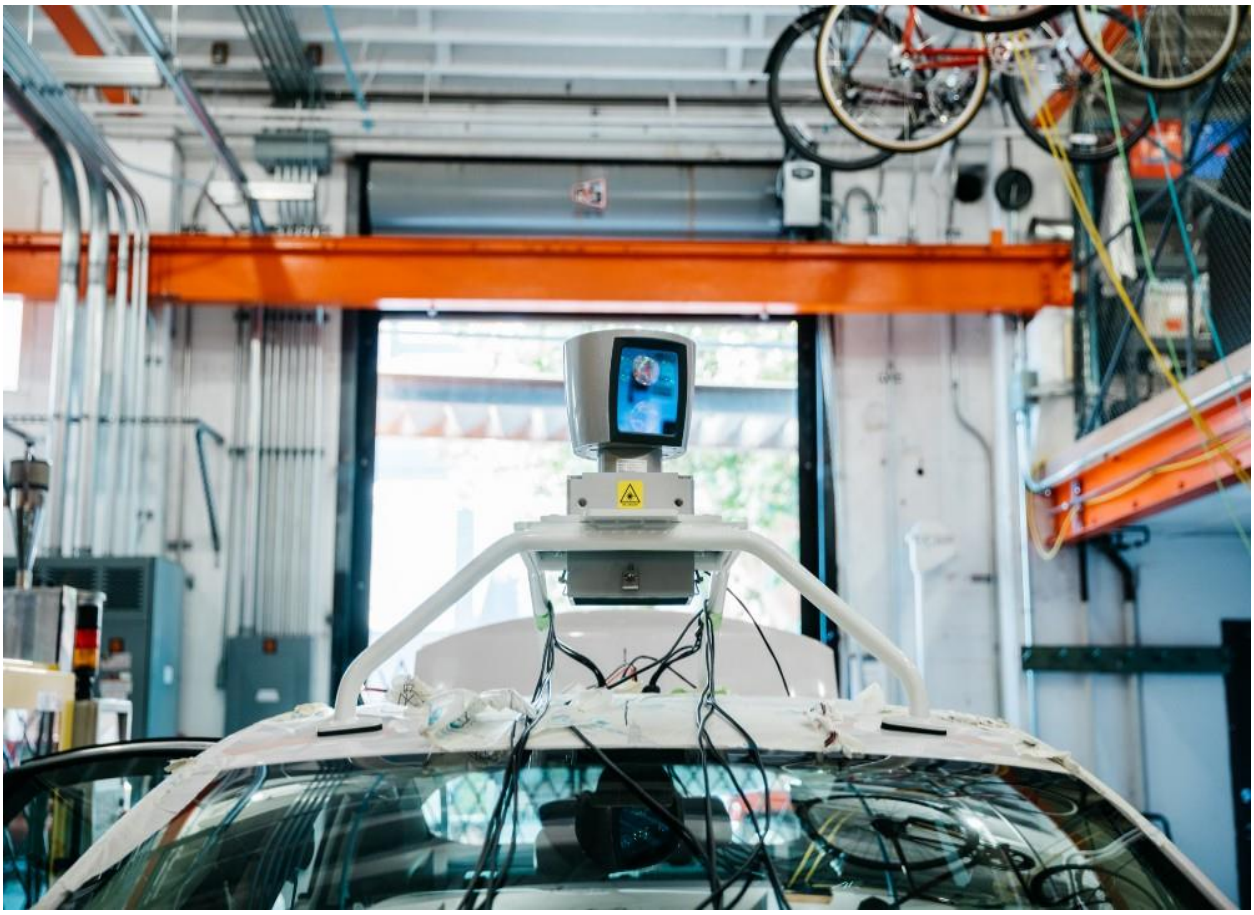
Senzorske tehnologije poput LiDAR-a ne ostavljaju prostora za tumačenje da li se objekt nalazi na kolniku emitirajući laserske zrake koje se reflektiraju od okolnih predmeta, a senzor ih ponovno otkriva. Hvataju izravne 3D podatke i tako preskaču međufazu pretvaranja 2D u 3D. Ako postoji prepreka ispred vozila, LiDAR senzori je pouzdano otkrivaju u ranoj fazi, utvrđuju točne dimenzije i, prije svega, udaljenost do vozila. 3D prikaz stvara se mjerenjem brzine svjetlosti i udaljenost koju njime prelazi što pomaže u određivanju položaja vozila s drugim okolnim objektima. 3D prikaz prati udaljenost između drugog koji prolazi pored vozila i bilo kojeg drugog vozila ispred njega. Pomaže u upravljanju kočnicama kako bi usporili ili zaustavili vozilo. Kad je put ispred nas čist, to omogućuje i ubrzanje vozila.

LIDAR omogućuje generiranje ogromnih 3D karata kojima potom možete predvidljivo kretati vozilom. Korištenjem LIDAR-a za mapiranje i kretanje okolinom možete unaprijed znati granice traka ili da se 500 metara ispred nalazi znak za zaustavljanje ili semafor. Ovakva je predvidljivost upravo ono što tehnologija poput autonomnih vozila zahtijeva i bila je veliki ra-

zlog za napredak u posljednjih 5 godina.

Međutim, vrsta predmeta koji se nalazi na putu vozila također može biti presudan čimbenik, jer nije svaki objekt prepreka koja zahtijeva da vozilo zakoči. Različite tehnologije senzora klasificiraju objekte na različite načine: LiDAR senzori, na primjer, prepoznaju skup točaka u podacima senzora. Na temelju veličine ovih nakupina, predmeti se mogu podijeliti u različite kategorije kao što su automobili, motocikli ili pješaci. Da bi se, na primjer, identificirala raznesena plastična vrećica kao takva i time bezopasna, analiza podataka kamere ponovno je korisna, što,

kao što je već opisano, koristi softver za prepoznavanje slike. Kamere su također potrebne za prepoznavanje putokaza, na primjer, jer LiDAR senzori ne bilježe boje.



Slika 8. Prikaz LIDAR senzora pričvršćenog na krov autonomnog vozila [24]

LiDAR je također ugrađen u novi sustav pod nazivom Pre-Scan. U Pre-Scan- u, laser skenira površinu ceste nekoliko stotina puta u sekundi. Te se informacije zatim unose u računalo automobila i obrađuju u djeliću sekunde, podešavajući pojedinačni ovjes na svakom kotaču.

Uz pomoć LiDAR-a autonomna vozila nesmetano putuju i izbjegavaju sudare otkrivajući prepreke ispred sebe. To poboljšava sigurnost putnika na putovanju i čini autonomne automobile manje podložnima nesrećama jer nema rizika od ljudskog nemara i brze vožnje.

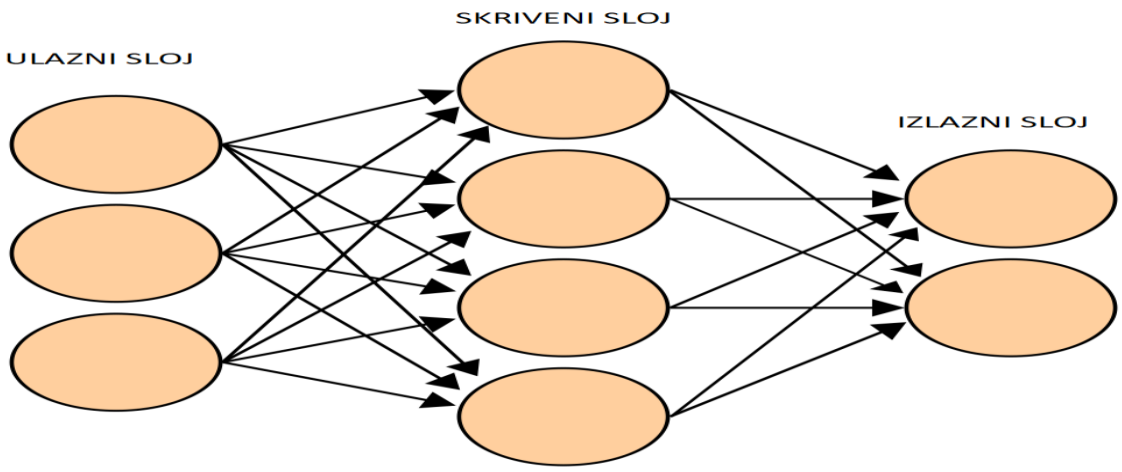
[24] https://towardsdatascience.com/how-to-make-a-vehicle-autonomous-16edf164c30f

3.4 Računala i neuronske mreže

Sva autonomna vozila, a u osnovi i sva moderna vozila, trebaju računalo za obradu svega što se događa s vozilom u stvarnom vremenu. Autonomna vozila zahtijevaju ekstremnu procesorsku snagu, pa umjesto tradicionalnih CPU-a za izračun koriste grafičke procesne jedinice ili GPU-ove. Zahvaljujući svojoj isplativosti i ogromnoj popularnosti, GPU se u nedavnoj prošlosti pojavio kao najdominantnija arhitektura čipova za tehnologiju autonomnih vozila. Sve veća složenost računalnog hardvera i zahtjevi za testiranje autonomnih automobila na stvarnim cestama jamče superiorne operativne platforme temeljene na AI koje bi predviđale potencijalne opasnosti tijekom vožnje.

Međutim, čak i najbolji GPU-ovi počeli su se pokazivati nedovoljnima za potrebe ekstremne obrade podataka viđene u autonomnim vozilima, pa je Tesla predstavio “Neural Network accelerator” čip ili skraćeno NNA. Da bismo opisali akcelerator neuronske mreže, poznat i kao "AI akcelerator", prvo moramo definirati neuronsku mrežu. Jednostavno rečeno, "**neuronska mreža**" samo je otmjeni naziv za skup algoritama koji izvode klasterizaciju i klasifikaciju podataka u programima strojnog učenja. Najosnovnija i najčešća vrsta arhitekture neuronske mreže naziva se “Feed- Forward” neuronska mreža (Slika 9.). Kod takve mreže informacija putuje u samo jednom smjeru od ulaza do izlaza. Sastoji se od ulaznog sloja i izlazni sloja, a između njih imamo nekoliko skrivenih slojeva. Ako imamo više od jednog skrivenog sloja, tada se ta mreža naziva dubokom neuronskom mrežom. [25]

[25] https://blogs.nvidia.com/blog/2021/04/12/gtc-keynote/



Slika 9. Primjer feed-forward neuronske mreže

Drugu vrstu neuronske mreže nazivamo **povratna**, odnosno "**Recurrent Neural Network**" skraćeno RNN. Ovo je složenija vrsta mreže, te se obično koristi u prepoznavanju govora i obradi prirodnog jezika. RNN-ovi izvode isti zadatak za svaki element niza, s tim da izlaz ovisi o prethodnim proračunima. Razlikujemo još i konvolucijske neuronske mreže, engl. Convolutional Neural Network, skraćeno CNN. CNN ima nekoliko slojeva kroz koje se podaci filtriraju u kategorije. CNN-ovi su se pokazali vrlo učinkovitima u područjima kao što su prepoznavanje slika, obrada jezika teksta i klasifikacija. Konvolucijska neuronska mreža sastoji se od ulaznog sloja, izlaznog sloja i skrivenog sloja koji uključuje više konvolucijskih slojeva, slojeva za spajanje, potpuno povezanih slojeva i slojeva za normalizaciju.

Akcelerator neuronske mreže je procesor koji je posebno optimiziran za rukovanje radnim opterećenjima neuronske mreže. Kao što naziv implicira, vrlo je učinkovit u obavljanju svog posla uzimanja podataka i klasterizacije te ih klasificira vrlo brzo. Ovi NNA imaju iznimnu moć obrade u stvarnom vremenu, te su sposobni za obradu slika u stvarnom vremenu.

Da bi vozilo uistinu moglo voziti bez kontrole vozača, u početku se mora provesti opsežna obuka za mrežu umjetne inteligencije (AI) kako bi mreža razumjela kako vidjeti, razumjela ono što vidi i donijela ispravne odluke u bilo kojoj zamislivoj prometnoj situaciji. Inženjeri "napajaju" mrežu stotinama tisuća slika - poput znakova zaustavljanja, znakova popuštanja, znakova ograničenja brzine, oznaka na cestama itd. - da bi je osposobili da iste prepozna na terenu.

Ekspertni sustavi rade spajanjem baze znanja s mehanizmom zaključivanja. Baza znanja je zbirka podataka, informacija i prošlih iskustava relevantnih za zadati zadatak i sadrži kako činjenično znanje (informacije široko prihvaćeno od strane ljudskih stručnjaka u tom području), tako i heurističko znanje (praksa, prosudba, procjena i pretpostavke). Stroj za zaključivanje koristi informacije sadržane u bazi znanja kako bi pronašao rješenja za probleme. To čini tako što:

- Višekratno primjenjuje pravila na činjenice dobivene iz ranije primjene pravila
- Dodavanjem novog znanja u bazu znanja kada se isto stekne
- Rješavanjem sukoba kada je za određeni slučaj primjenjivo više pravila

Da bi preporučio rješenje, mehanizam za zaključivanje koristi i lanac prema naprijed i unatrag. Usmjeravanje unaprijed odgovara na pitanje "Što se može dalje dogoditi?" i uključuje identificiranje činjenica, slijeđenje lanca uvjeta i odluka i pronalaženje rješenja. U kontekstu autonomnih vozila, činjenično znanje sastoji se od pravila puta kao i postupaka upravljanja vozilom. Heurističko znanje sastoji se od kolektivnih prošlih iskustava iskusnih vozača koji informiraju o njihovom donošenju odluka - na primjer, razumijevanje postojanja zaleđenih dijelova ceste i posljedično smanjenju brzine i omogućavanju povećanja zaustavnog puta

Na svakoj razini autonomne vožnje, procesorska snaga potrebna za rukovanje svim podacima brzo se povećava. U pravilu se može očekivati 10x povećanje obrade od jedne do druge razine. Računalne performanse autonomnog automobila jednake su nekim od platforma s najvišim performansama koje su bile nemoguće do prije nekoliko godina. Predviđa se da će autonomno vozilo sadržavati više redaka koda nego bilo koja druga softverska platforma koja je stvorena do danas. Očekuje se da će tipično vozilo sadržavati više od 300 milijuna redaka koda i sadržavat će više od 1 TB (terabajt) prostora za pohranu, a bit će mu potrebna propusnost memorije veća od 1 TB u sekundi kako bi podržala računske performanse potrebne za autonomnu vožnju.

AI sustav autonomnog automobila zahtjeva kontinuirani, neprekinuti tok podataka i uputa kako bi donosio odluke u stvarnom vremenu na temelju složenih skupova podataka. Uspješna autonomna vozila danas postoje na cesti, međutim uspjeh mnogih do sada stvorenih vozila rezultat je neprekidne vožnje istom rutom tijekom mnogih dana, gdje nauče sve detalje

rute i generiraju mape visoke razlučivosti, zatim se koristi kao ključni dio samonavigacijskog sustava. Uz manje oslanjanja na potrebu prepoznavanja rute, pozornost autonomnog računala može se posvetiti prometu, pješacima i ostalim potencijalnim opasnostima u stvarnom vremenu. Ovaj općenito ograničeni opseg rada naziva se "geo-ogradom" i odražava pristup koji prihvaćaju dosadašnja autonomna vozila. Iako "geo-ograda" može dovesti do rješenja koje može funkcionirati na ograničenoj ruti, autonomno vozilo s velikim oslanjanjem na "geo-ogradu" u jednom dijelu svijeta možda neće funkcionirati dobro kao u drugom.

Istraživači i profesionalci primjenjuju tehnologiju računalnog vida na autonomna vozila kako bi vožnja bila sigurnija i za putnike i za pješake. Tehnologija se u autonomnom vozilu može koristiti na više načina. Omogućujući autonomnim vozilima hvatanje vizualnih podataka u stvarnom vremenu. Kamere povezane s takvim vozilima mogu snimati snimke uživo i omogućiti računalnom vidu stvaranje 3D mapa. Koristeći ove karte, autonomna vozila mogu bolje razumjeti svoju okolinu dok uočavaju prepreke na svom putu i odlučuju se za zamjenske rute s 3D kartama. Autonomna vozila mogu predvidjeti nesreće pomoću 3D karata i mogu trenutno aktivirati zračne jastuke za zaštitu putnika. Ovo rješenje autonomne automobile čini sigurnijima i pouzdanijima. Stoga tehnologija može pomoći u izradi sigurnih autonomnih vozila kako bi se izbjegle nesreće i zaštitili putnici. [26]

Tehnologija klasificiranja I detekcije objekata pomaže autonomnim vozilima da klasificiraju i otkriju različite predmete koji se nalaze u njihovom okruženju. Vozilo može koristiti LiDAR senzore i kamere, a prvi može koristiti pulsirajuće laserske zrake za mjerenje udaljenosti. Dobiveni podaci mogu se kombinirati s 3D mapama za uočavanje objekata poput semafora, vozila i pješaka. Ova tehnološki orijentirana vozila obrađuju takve podatke u svojim računalima kako bi donosila odluke u stvarnom vremenu. Dakle, računalni vid omogućit će autonomnim vozilima prepoznavanje prepreka i izbjegavanje sudara i nesreća. [27]

---

[26] *National Highway Traffic Safety Administration. "NCSA Publications & Data Requests." 2017, crashstats.nhtsa.dot.gov/#/.*

[27] A. Brunetti, D. Buongiorno, G. Trotta, V. Bevilacqua: Computer vision and deep learning techniques for pedestrian detection and tracking: a survey Neurocomputing, 300 (2018)

Tehnologija računalnog vida može prikupiti velike skupove podataka pomoću kamera i senzora, uključujući informacije o lokaciji, prometne uvjete, održavanje cesta, gužve i druge. Ovi detaljni podaci mogu pomoći vozilima koja se samostalno voze da iskoriste svjesnost o situaciji i što prije donesu vitalne odluke. Ovi se detalji mogu dalje koristiti u obuci modela dubokog učenja. Primjerice, tisuću slika prometnih signala prikupljenih računalnim vidom može se koristiti u treningu modela za otkrivanje prometne signalizacije tijekom vožnje. Uz to, može pomoći autonomnim vozilima u razvrstavanju različitih vrsta predmeta. [28]

Umjetna inteligencija (AI) se u kontekstu autonomnih vozila (AV) fokusira na percepciju okoliša i automatizirane odgovore na to okruženje, istodobno izvršavajući primarni cilj da se vozilo sigurno odveze od polazišta do odredišta. U nastavku razmatramo dvije funkcije AI u kontekstu autonomnih vozila. Autonomna vozila moraju biti sposobna "vidjeti" svijet oko sebe kako bi sigurno putovale od točke A do točke B. Da bi to učinile, moraju biti sposobne prepoznati sve elemente koji zajedno čine transportni sustav, uključujući ostala vozila, pješake i bicikliste, kao i okoliš vozila, poput infrastrukture kolnika, zgrada, kontrola raskrižja, znakova, oznaka na kolnicima i vremenskih uvjeta. Siguran rad AV zahtijeva povezanost vozila i ostalih elemenata transportnog sustava. Inženjeri su identificirali pet ključnih vrsta povezivanja:

- V2I: Vozilo do infrastrukture (ceste, semafori, oznake kilometara, itd.)
- V2V: Vozilo do vozila (ostale AV)
- V2C: Vozilo u oblak (podaci za napajanje navigacijskim sustavima, zabavnim sustavima itd.)
- V2P: Vozilo prema pješaku (pasivna komunikacija od pješaka do AV)
- V2X: Vozilo do svega (bicikli, zgrade, drveće itd.)

[28] A. Brunetti, D. Buongiorno, G. Trotta, V. Bevilacqua: Computer vision and deep learning techniques for pedestrian detection and tracking: a survey Neurocomputing, 300 (2018)

4. Sigurnosno-komunikacijski zahtjevi autonomnih vozila

Autonomna vožnja predstavlja nekoliko ključnih tehničkih izazova. Jedan od tih izazova je sposobnost rukovanja i analize ogromnih količina podataka. Primjer je sve veći broj senzora u vozilu i izvan njega. Drugi primjer je ogroman broj moćnih računala koji obrađuju upravljačke funkcije visoke razine i algoritme strojnog učenja. Uz to, automobil će morati biti u mogućnosti obrađivati bežične (OTA) tokove podataka za **vozilo-do-zgrade** (V2B), **vozilo-do-vozila** (V2V), **vozilo-do-infrastrukture** (V2I), **vozilo do korisnika** (V2U) i **vozilo do komunikacijske infrastrukture** (V2C) pouzdano i trenutno. Te se funkcije zajedno mogu nazvati **V2X**.

Slika 10. Prikaz bitnih značajka koje definiraju sigurnosno- komunikacijske zahtjeve

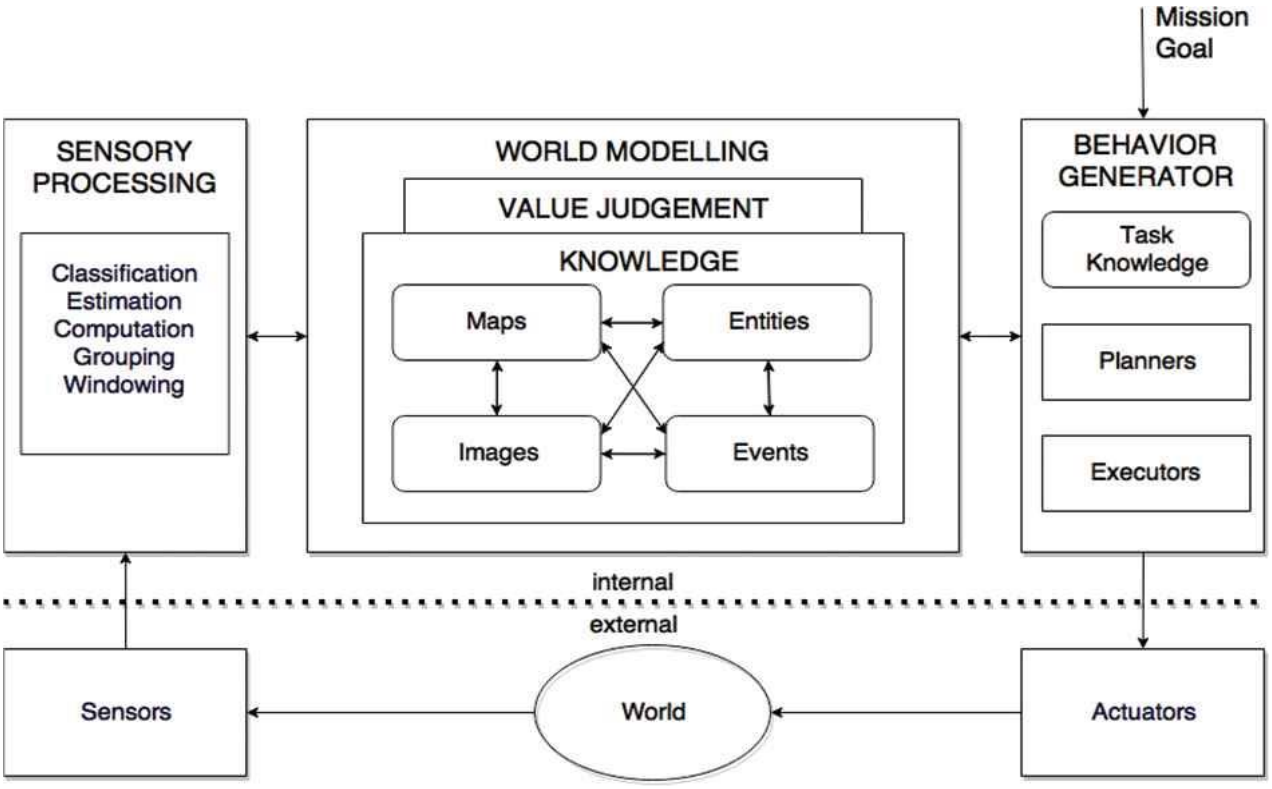
4.1 Arhitektura softvera autonomnih vozila

Nova će vozila uskoro dobiti arhitekture koje organiziraju klastere visokih performansi u funkcionalnim domenama, kao što se vidi na slici 11. Te su domene povezane hijerarhijski putem središnjeg pristupnika u strukturi podataka velike brzine na glavnoj mreži i grupiraju senzore i aktuatore. Autonomna vožnja sve više zahtijeva baziranje na pouzdanijim mrežnim strukturama. Dizajn softverske arhitekture za autonomna vozila analogan je dizajnu inteligentnog, upravljačkog sustava u stvarnom vremenu ili robota. Dugo je vremena u AI zajednici dominiralo stajalište da bi se sustav upravljanja autonomnim robotima trebao sastojati od tri funkcionalna elementa: senzorskog sustava, sustava planiranja i izvršnog sustava.[29]

Ovo je gledište dovelo do sveprisutne paradigme osjetilnog plana-čina. Za planiranje, sustav obično održava unutarnje stanje pripravnosti, što mu omogućuje pozicioniranje u okruženju i planiranje sljedećih akcija. Budući da ovaj model mora biti ažuran i točno odražavati okruženje u kojem robot djeluje, možda će trebati puno informacija. Kako operacijsko okruženje postaje složenije, složenost interne operativnosti također se povećava, povećavajući vrijeme potrebno za planiranje sljedećih koraka. Stoga, u okruženjima koja se brzo mijenjaju, novi planovi mogu biti zastarjeli prije njihove primjene. Štoviše, neočekivani ishodi izvršenja matičnog plana mogu uzrokovati izvršenje sljedećih koraka plana u odgovarajućem kontekstu i dovesti do neočekivanih ishoda.

Promišljajući sustavi djeluju na temelju svojeg unutarnjeg predstavljanja okoliša koji ga okružuje, a reaktivni sustav ispunjava ciljeve refleksivnim reakcijama na promjene u okolišu. Reaktivni sustavi ili sustavi temeljeni na ponašanju sposobni su brže reagirati na promjenjivu okolinu, ali manje razmišljajući o istoj.[30]

[29] P. Maes, "Behavior-based artificial intelligence," in Proceedings of the Fifteenth Annual Meeting of the Cognitive Science Society, pp. 74–83, 1993.
[30] N. Muscettola, G. A. Dorais, C. Fry, R. Levinson, and C. Plaunt, "Idea: Planning at the core of autonomous reactive agents," in NASA Workshop on Planning and Scheduling for Space, 2002.



Slika 11. Model referentne arhitekture inteligentnih upravljačkih sustava u stvarnom vremenu[31]

Promatrajući razvoj autonomnih vozila kroz ove prizme, možemo vidjeti da vozila zahtijevaju reaktivne i promišljene dijelove. Održavanje unaprijed definirane putanje i udaljenosti od predmeta oko vozila primjer je reaktivnog sustava koji bi trebao raditi s visokom frekvencijom i biti što brži kako bi se prevladale bilo kakve promjene u okolišu. U ovom slučaju uzaludno je održavati složenu predstavu okolnog okoliša. Međutim, mehanizam donošenja odluka odgovoran, na primjer, za pretjecanje vozila ispred, primjer je promišljenog sustava.

Gat i Bonnasso raspravljaju o ulozi unutarnjeg stanja i uspostavljaju ravnotežu između reaktivnih i promišljenih komponenata unutar sustava. U njihovom su prijedlogu funkcionalne komponente klasificirane na temelju njihova pamćenja i znanja o unutarnjem stanju u: nema znanja, znanja iz prošlosti ili znanja o budućnosti - što rezultira u tri sloja funkcionalnih komponenata. Međutim, njihov model ne precizira kako ili da li se znanje može podijeliti između

[31] https://www.atlantis-press.com/journals/jase/125934832/view

slojeva. Štoviše, nije jasno kako i sadrže li bilo koje komponente znanje o prošlim, budućim i drugim statičkim podacima. [32]

Bolji prijedlog koji premošćuje jaz između reaktivnih i promišljajućih komponenti je referentna arhitektura NIST-a u stvarnom vremenu (RCS). Ova arhitektura ne razdvaja komponente temeljene na memoriji, već gradi hijerarhiju temeljenu na semantičkom znanju. Dakle, komponente niže u hijerarhiji imaju ograničeno semantičko razumijevanje i mogu generirati ulaze za više komponente, produbljujući njihovo semantičko znanje i razumijevanje. Štoviše, RCS nema vremenskih ograničenja za znanje komponente. Mogu se čuvati statične ili dinamičke informacije o prošlosti, sadašnjosti ili budućnosti. Iako sve komponente održavaju world model, to može biti jednostavno poput referentnih vrijednosti s kojima se ulaz mora usporediti.[33]

U središtu kontrolne petlje za RCS čvor je prikaz vanjskog svijeta - svjetskog modela - koji pruža mjesto za fuziju podataka, djeluje kao međuspremnik između percepcije i ponašanja te podržava senzornu obradu i generiranje ponašanja. Ovisno o složenosti zadatka za koji je čvor odgovoran, složenost svjetskog modela raste. Za najjednostavnije zadatke svjetski model može biti vrlo jednostavan, kao što je slučaj s sustavom leptira za gas koji ima samo znanje o brzini automobila i ulazima koje prima s papučice ubrzanja. Za složene zadatke, poput planiranja odredišta, svjetski model mora uključivati složene informacije kao što su karte za operativnu domenu, prometne informacije u stvarnom vremenu itd.

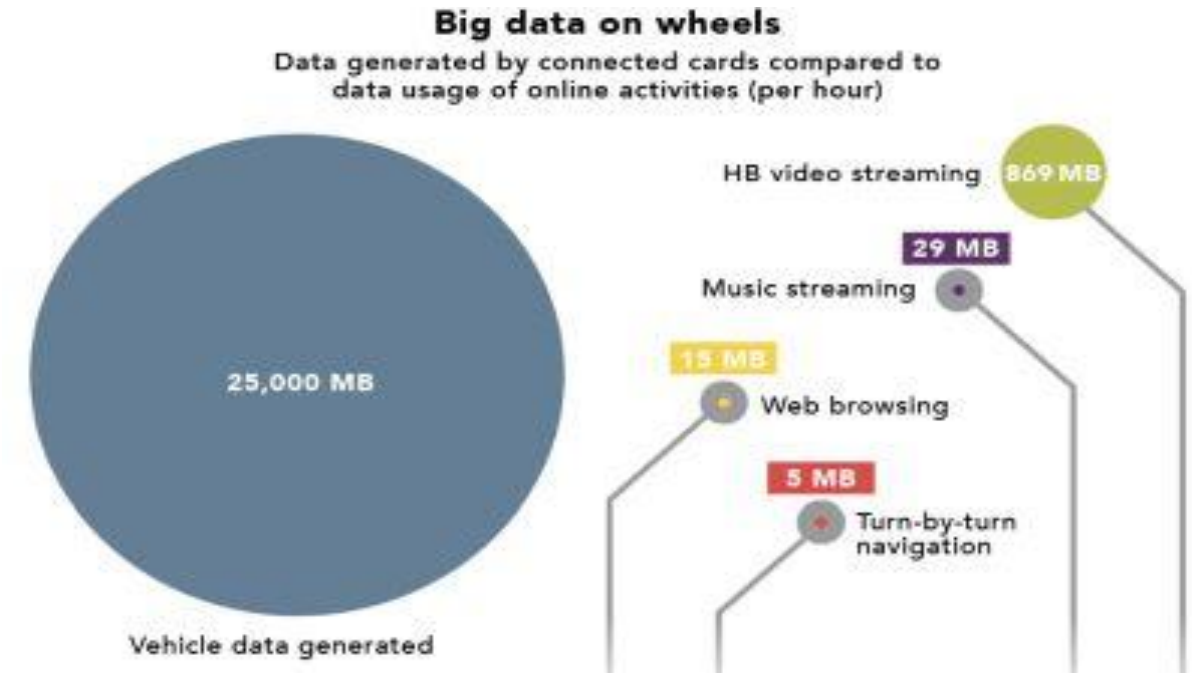
4.2 Prijenos podataka velikim brzinama

Kako raste broj povezanih automobila, tako će rasti i mjera u kojoj oni proizvode, prenose i primaju podatke. Količina podataka koja se prenosi povezanim vozilom (u oblak i iz njega) iznosi približno 25 GB podataka/ sat (Slika 14) i predviđa da će se ta brojka povećati na gotovo 500 GB podataka / sat nakon što vozila uistinu budu autonomna.

[32] E. Gat and R. P. Bonnasso, "On three-layer architectures," Artificial intelligence and mobile robots, vol. 195, p. 210, 1998.

[33] J. S. Albus, "The NIST real-time control system (RCS): an approach to intelligent systems research," Journal of Experimental & Theoretical Artificial Intelligence, vol. 9, no. 2-3, pp. 157–174, 1997.

Današnje mreže u vozilu zapravo koriste kombinaciju nekoliko različitih protokola umrežavanja podataka. Neki od njih postoje desetljećima. Među njima je regulator mrežnih područja (CAN) koja upravlja funkcijama pogonskog sklopa i aktuatora, lokalna interkonektna mreža (LIN) koja pretežno rukuje vremenski osjetljivim aplikacijama poput kontrole klime, ambijentalne rasvjete, podešavanja sjedala i slično, medijski orijentirani transport sustava (MOST) za infotainment; i FlexRay za antiblokirno kočenje, elektronički servo upravljač i funkcije stabilnosti vozila.



Slika 12. Prikaz podataka koje kreira povezano vozilo na mrežu, te njihovu količinu [34]

Mrežna struktura koja se koristi danas u vozilima kreće prema varijanti onoga što se naziva arhitekturom zasnovanom na domeni (svaki proizvođač automobila ima svoju arhitekturu, ali glavni koncept je često sličan). Tamo gdje su starije mreže vozila imale specifične ECU-ove i sabirničke sustave specifične za aplikaciju, arhitekture domena karakteriziraju različite domene za svaku ključnu funkciju: jedna ECU-a i upravljanje tijelom za upravljanje mrežom, jedna ECU, mreža za info-zabavu, jedna za telematiku, jedna za pogonski sklop, i tako dalje. Barem zasad, te domene još uvijek koriste kombinaciju različitih mrežnih protokola (CAN, LIN i tako dalje).

[34] https://www.microcontrollertips.com/what-high-speed-data-means-for-connected-vehicles/

Kako mreže postaju složenije, ovaj pristup zasnovan na domeni postaje sve manje učinkovit. Dakle, doći će do migracije s arhitektura temeljenih na domeni prema tipu koji se naziva zonska arhitektura. **Zonska arhitektura** povezuje podatke s različitih tradicionalnih domena na istu ECU, na temelju lokacije (zone) ECU-a u vozilu. Ova shema uvelike smanjuje količinu korištenja žice, djelomično jer će se mnoge funkcije s kojima se sada radi s diskretnim ožičenjem prebaciti na Ethernet tehnologiju.

Za razliku od ostalih mrežnih protokola u vozilu, Ethernet ima dobro definiran razvojni plan za postizanje većih brzina. Suprotno tome, tradicionalni automobilski protokoli poput CAN i LIN nalaze se na mjestu gdje planirane aplikacije premašuju svoje mogućnosti bez jasnog puta nadogradnje za rješavanje problema. Očekivanja su da će se većina podataka u vozilima prenositi putem Etherneta. Stoga je plan za jedinstvenu homogenu mrežu u cijelom vozilu. Ova mreža u vozilu bit će prilagodljiva tako da će moći obrađivati funkcije koje zahtijevaju veće brzine (na primjer 10G) s ultra niskom latencijom, ali ujedno i sporije funkcije. Dizajneri će odabrati fizički sloj Etherneta za određene funkcije prema zahtjevima propusnosti. Tako bi senzori slike bogati podacima, poput radara i lidara, mogli koristiti sučelje od 1 Gbps, gdje bi senzorima s niskom brzinom prijenosa podataka trebala biti potrebna samo veza od 10 Mbps.

Zonske će arhitekture koristiti Ethernet preklopnike za upravljanje podacima za sve različite aktivnosti domene. Različite domene podataka spojit će se na lokalne prekidače, a okosnica Etherneta tada bi agregirala podatke. Na taj način mreža može koristiti iste temeljne protokole kako bi podržala upotrebu različitih brzina.

Sljedeći trend koji utječe na povezana vozila je prelazak na **5G mreže.** Glavni telekomunikacijski operateri započeli su s aktiviranjem bežičnih mreža pete generacije (5G) u gradskim područjima. Pojava 5G bežičnih podataka mogla bi inteligentnu i autonomnu vožnju podići na sljedeću razinu omogućujući brže brzine prijenosa podataka i sigurnu povezanost od vozila do vozila (V2V) i od vozila do infrastrukture (V2X). Predviđen za široko prihvaćanje u roku od nekoliko godina, 5G će zahtijevati kontinuirani napredak u razvoju moćne mrežne infrastrukture i tehnologija obrade u vozilu kako bi se osigurala pouzdana brzina signala s ultra niskom propusnošću kašnjenja.

Da bismo objasnili što 5G može značiti za automobilsku povezanost, moglo bi biti korisno navesti stvarne primjere 5G mogućnosti koje su sada u fazi prototipa. Jedan od takvih projekata je AutoAir koji se testira na poligonu Millbrook u Velikoj Britaniji. Tamošnji istraživači postavili su bazne stanice, antene i drugi hardver kako bi stvorili scenarije koji uključuju održavanje veze od 1 Gbps na vozila koja brzinom prelaze do 160 mph. Još jednu implementaciju 5G nazvanu Nevidljivo-vidljivo opisao je CES 2019 Nissan. Koristi brzu povezanost kako bi vidio zavoje i upozorio putnike na potencijalne opasnosti kao što su prepreke na cesti ili pješaci zaklonjeni vozilima. Slično tome, Ford Motor surađuje s Vodafonom na sustavu koji koristi 5G da upozori automobile na približavanje hitnim vozilima.

Ova brza automobilska rješenja zahtijevaju razinu stručnosti i inženjerstva koja premašuje razinu mnogih drugih aplikacija. Velik dio složenosti dizajna dolazi od napora da se ostvare bolje performanse konektora, kabelskih sklopova i modula koji imaju male otiske. Više nije dovoljno da hardver za povezivanje karakteriziraju jednostavni parametri kao što su otpornost na kontakt i otpornost na koroziju. Hardver koji obrađuje podatke velike brzine mora se baviti zaštitom od elektromagnetskih smetnji i mora se karakterizirati u smislu slabljenja, povratnog gubitka, pretvorbe načina, preslušavanja, impedancije i drugih problema koji mogu utjecati na prijenos signala. Mnogo se ulaže u specificiranje konektora koji imaju mogućnost pouzdanog isporučivanja signala velike brzine, širokopojasne širine i velike snage do i od svakog senzora u vozilu.[35]

4.3 Sigurnost podataka

Zakon o zaštiti podataka od posebne je važnosti u kontekstu povezane i autonomne mobilnosti. To je zato što je širina podataka koji se automatski prikupljaju vrlo velika. Nisu svi prikupljeni podaci zapravo potrebni iz tehničke perspektive kako bi se omogućila povezana i autonomna vožnja. To se odnosi, na primjer, na podatke koje pojedinačni vozač/ korisnik unosi u svrhu info-zabave ili komfornih postavki. S druge strane, prikupljaju se podaci za usluge Vozilo-do-X i prediktivna dijagnostika te sustavi poput eCall-a, zajedno s radnim vrijednostima vozila,

[35] https://www.machinedesign.com/mechanical-motion-systems/article/21837614/5gs-important-role-in-autonomous-car-technology

agregiranim podacima o vozilu koji se generiraju u vozilu, poput memorije kvarova, broja kvarova, prosjeka brzina i potrošnja, te tehnički podaci, npr. podaci generirani senzorima.

Od svih ovih podataka velik će se dio smatrati osobnim podacima, tako da će se Opća uredba o zaštiti podataka (GDPR) (i u budućnosti, na primjer, Uredba o e-privatnosti, koja još nije stupila na snagu), primjenjivati na povezana i autonomna vozila. Istodobno, ne očekuje se da obradu svih ovih podataka provodi jedan kontrolor podataka koji se mora pridržavati zahtjeva zaštite podataka za prikupljanje i upotrebu osobnih podataka - radije će različiti kontrolori podataka imati pristup različitim podacima.

U tom kontekstu, potrebno je razjasniti brojna pravna pitanja, poput toga tko određuje svrhe i sredstva obrade podataka, postoji li nekoliko zajedničkih kontrolora ili stranaka koje djeluju prema uputama druge strane. Primjerice, proizvođači, osiguravatelji i davatelji automobila mogu zajednički upravljati kad zajednički određuju sredstva i svrhe obrade određenih osobnih podataka.

U ranoj fazi razvoja svojih proizvoda i poslovnih modela, davatelji povezanih i autonomnih vozila i sustava stoga će morati analizirati koji zahtjevi zaštite podataka moraju biti ispunjeni kako bi postupili u skladu sa zakonom i stvorili povjerenje u njih i nove oblike mobilnosti sa stajališta zakona o zaštiti podataka.

Odlučujući faktor za primjenjivost zakona o zaštiti podataka jest obrada osobnih podataka. "Osobni podatak" znači bilo koji podatak koji se odnosi na utvrđenu ili utvrdivu fizičku osobu. Ovaj pravni koncept treba shvatiti vrlo široko. Kao rezultat toga, fizička osoba koja se može identificirati treba se definirati kao ona koja se može izravno ili neizravno identificirati, posebno udruživanjem s identifikatorom kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili jedna ili više specifičnih karakteristike.

Klasifikacija ovisi o tome tko zapravo prikuplja podatke. Na primjer, operater voznog parka ima različite mogućnosti dodijeljivanja činjeničnih podataka, kao što su podaci o kretanju pojedinih vozila, određenim osobama, budući da on zna koja su vozila dodijeljena kojoj osobi. Stoga su za operatora podaci o transakcijama redovito povezani s osobom, dok, na primjer,

mehanička radionica čita podatke o transakcijama radi održavanja vozila, ali - ovisno o okolnostima pojedinačnog slučaja - često ih ne može dodijeliti određena osoba.

"Dizajn privatnosti" je zakonski zahtjev prema GDPR-u i utječe na početak postupka razvoja proizvoda. Kao rezultat toga, proizvođači vozila trebali bi to posebno uzeti u obzir. Dizajn privatnosti zahtijeva poduzimanje odgovarajućih tehničkih i organizacijskih mjera, poput pseudonimizacije, kako bi se učinkovito provodila načela zakona o zaštiti podataka, po-put minimiziranja podataka. Stoga su prikladne metode tehnološkog dizajna osigurane da se uvaže zahtjevi GDPR-a i zaštite prava dotičnih subjekata podataka.

Načela „privatnost prema zadanim postavkama“ i „privatnost prema dizajnu“ od posebne su važnosti za osiguravanje, putem unaprijed postavljenih postavki prilagođenih zaštiti podataka, da se obrađuju samo osobni podaci čija je obrada potrebna za određenu svrhu. To se odnosi na količinu prikupljenih osobnih podataka, opseg obrade, razdoblje pohrane i dostupnost. Idealno bi bilo da aplikacije za povezanu i autonomnu mobilnost budu dizajnirane od samog početka tako da se obrađuje što manje osobnih podataka za odgovarajuće svrhe. Također treba napomenuti da GDPR također postavlja vrlo dalekosežna pravila za dokumentaciju i organizaciju poštivanja zaštite podataka.

4.4 Pouzdanost prikupljenih podataka

Pouzdano prepoznavanje i prijenos podataka u svim uvjetima, posebno u surovim uvjetima, obvezno je. Rješenje je vrlo robusni automobilski sustavi povezivanja koji su najmanje vjerojatni da će propasti čak i nakon tisuća i tisuća sati operacije. Proizvođači bi se trebali udružiti s kompetentnim i iskusnim partnerom koji razvija cjelovita rješenja sustava koristeći pristup holističkog dizajna sustava. Pristup bi trebao obuhvaćati dizajn mehaničkih i električnih sustava, usklađena tehnološka rješenja i rješenja za automatizaciju te nove proizvodne postupke.

Isprava o sigurnosti autonomnih vozila trajala je od njihovog nastanka, uglavnom okružujući sposobnost automobila da umjetnim inteligencijama precizno osjeti i na odgovarajući način reagira na svoje neposredno okruženje. Unatoč očekivanjima mnogih da će autonomni automobili biti manje opasni od svojih “kolega” s ljudima za volanom, ta će zabrinutost rasti kako

se približavamo uvođenju ovih vozila. Iako će umjetna inteligencija pridonijeti sigurnosti vozila, najozbiljniji rizik za uspjeh autonomne tehnologije mogao bi doći iz sve fragmentiranije prirode samog tržišta automobila i transporta.

U čitavoj automobilskoj industriji suparničke tvrtke koje su pioniri u tehnologiji autonomnih vozila inženjerski su automobili s ugrađenim senzorima i komunikacijskim sustavima koji su dizajnirani izolirano, s ciljem da se osigura kompatibilnost. Dizajnirani i izrađeni od različitih pojedinačnih operatera, ovi će modeli vjerojatno biti ograničeni na rad uz vozila proizvedena na isti način. Sustavi su tako dizajnirani da upravljaju pojedinačnim automobilom, a ne 'flotom' vozila koja će putovati našim cestama. Ovaj potencijalni rizik mogao bi se izbjeći pristupom razvoju sustava mobilnosti koji se temelji na boljoj suradnji između tvrtka. Povezani vozni park bez vozača moći će i trebati se oslanjati na ‘mudrost gomile’ kako bi naučili o događajima uživo na način koji današnja vozila nisu u stanju učiniti. Pojedinačni automobili imaju mogućnost skupljanja podataka u stvarnom vremenu o opasnostima na cesti od drugih vozila na cesti. Takav bi sustav trebao objediniti bogatu nacionalnu bazu podataka svih sudionika u prometu i cestovne infrastrukture, s jednakom pokrivenošću u cijeloj zemlji. Da bi se osigurala korist za sve, morat će biti održiv u inozemstvu, a što je još kritičnije, mora biti neutralan prema dobavljačima. Svi povezani automobili i automobili bez vozača moraju biti sposobni raditi kao pokretna flota "geodeta", što zajednički doprinosi sigurnosti svih ostalih sudionika u prometu.

Jedinstveni standard za komunikaciju između autonomnih vozila, tako da lokalne vlasti mogu nadzirati i upravljati svim modelima automobila bez vozača jedno je od potencijalni rješenja takvih problema. Buduća cestovna sigurnost zahtijevat će autonomna vozila kako bi osigurala međusobnu sigurnost i presijecala se s drugim načinima prijevoza s potencijalom da donesu šire ekološke i društvene koristi, poput poboljšanja kvalitete zraka.

5. Procjena rizika autonomnih vozila

U bilo kojem sustavu upravljanja cyber sigurnošću, procjena i ublažavanje svih ranjivosti ključna je odgovornost osiguravanja da proizvod funkcionira na maksimalno sigurnoj razini. Skeniranje ranjivosti nije provjera na jednom mjestu, već bi se trebala provoditi na svakoj razini procesa razvoja proizvoda kako bi se omogućilo maksimalno ublažavanje i sveobuhvatna analiza dodatnih prijetnji.

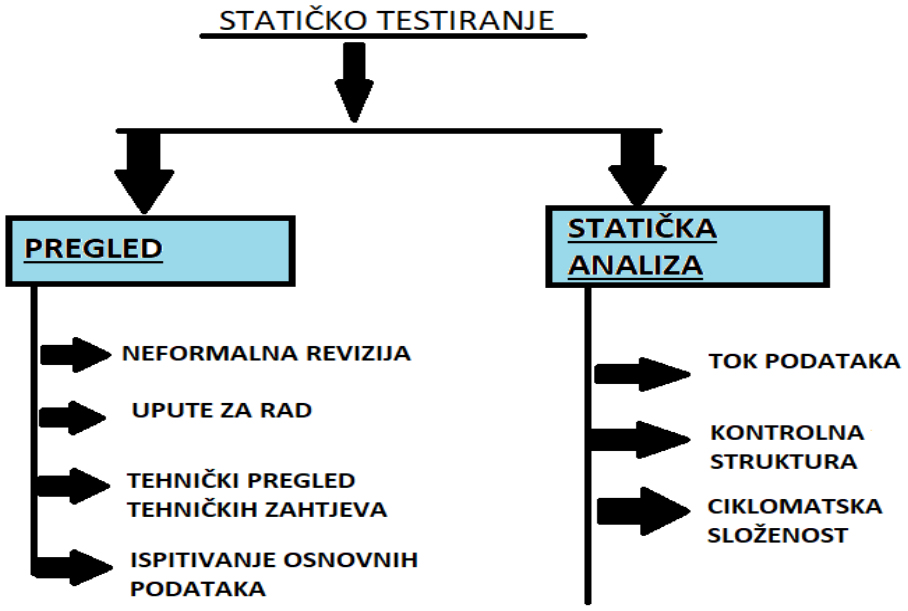
5.1 Statičko testiranje softvera

Statičko testiranje softvera testira izvorni ili objektni kôd bez njegovog izvođenja radi pronalaženja i uklanjanja pogrešaka ili nejasnoća. Obično se to radi u ranim fazama razvoja. Ovaj je korak presudan jer može otkriti glavne probleme poput curenja podataka, prekoračenja kapaciteta međuspremnika i odstupanja od standarda. Budući da se testiranje vrši u ranoj fazi, može se zaštititi od povećanja vremenskih rokova prilikom razvoja i omogućiti da se u kasnijim fazama razvoja pronađe manje problema, što često može biti puno skuplje i dugotrajnije za popravljanje.

Sastoji se od dva dijela:

- Pregled - Obično se koristi za pronalaženje i uklanjanje pogrešaka ili nejasnoća u dokumentima kao što su zahtjevi, dizajn, test slučajevi itd.
- Statička analiza - kod koji su napisali programeri analizira se (obično pomoću alata) na strukturne nedostatke koji mogu dovesti do nedostataka.

Pregled softvera (Slika 13.) uključuje **neformalnu reviziju** pri kojoj kreator stavlja sadržaj pred publiku i svatko daje svoje mišljenje te se tako nedostaci prepoznaju u ranoj fazi. **Upute za rad** prilikom koji se prolazi kroz rad programa sa pažnjom na funkcionalnim zahtjevima. U osnovi obavlja iskusna osoba ili stručnjak kako bi provjerio nedostatke kako ne bi došlo do daljnjih problema u fazi razvoja ili ispitivanja. Tehnički pregled s pozornošću na tehničkim zahtjevima podrazumijeva provjeru međusobnih dokumenata radi otkrivanja i otklanjanja nedostataka. U osnovi se to radi u timu kolega.



Slika 13. Prikaz statičkog testiranja softvera

Statička analiza uključuje ocjenu kvalitete koda koju su napisali programeri. Za analizu koda i usporedbu istog sa standardom koriste se različiti alati. Također pomaže u sljedećem utvrđivanju sljedećih nedostataka:

a) Neiskorištene varijable
b) Mrtvi kod
c) Beskonačne petlje
d) Varijabla s nedefiniranom vrijednošću
e) Pogrešna sintaksa

Statička analiza se sastoji od 3 dijela. Obrade **toka podataka**, to je softverska paradigma koja se temelji na ideji razdvajanja računskih aktera u faze (cjevovode) koje se mogu istodobno izvršavati. Protok podataka također se može nazvati obrada toka ili reaktivno programiranje. **Kontrolna struktura** je u osnovi način na koji se izvršavaju izrazi ili upute. Naglasak na

eksplicitnom tijeku upravljanja razlikuje imperativni programski jezik od deklarativnog programskog jezika. Unutar imperativnog programskog jezika, izraz tijeka upravljanja je iskaz koji rezultira odabirom kojeg od dva ili više putova treba slijediti. **Ciklomatska složenost** mjerenje je složenosti programa koje je u osnovi povezano s brojem neovisnih putova u grafikonu kontrolnog toka programa.

5.2 Dinamičko testiranje softvera

Dinamičko testiranje jedan je od najvažnijih dijelova softverskog testiranja koji se koristi za analizu dinamičkog ponašanja koda. Dinamičko testiranje softvera radi se tako da se dodaju ulazne vrijednosti i zatim provjerava očekuje li se izlaz primjenom određenog testnog slučaja koji se može obaviti ručno ili postupkom automatizacije.Dinamičko testiranje može se izvršiti kada se kôd izvršava u okruženju vremena izvođenja.

To je postupak provjere valjanosti u kojem se izvode funkcionalna ispitivanja [testiranje prihvatljivosti jedinice, integracije, sustava i korisnika] i nefunkcionalna ispitivanja [ispitivanje performansi, upotrebljivosti, kompatibilnosti, oporavka i sigurnosti]. Kao što znamo da je statičko testiranje postupak provjere, dok je dinamičko testiranje postupak provjere valjanosti, a zajedno nam pomažu u isporuci isplativog kvalitetnog softverskog proizvoda. Lako možemo razumjeti kako implementirati dinamičko testiranje tijekom STLC-a [Životni ciklus testiranja softvera] ako uzmemo u obzir karakteristike dostupne dinamičkim ispitivanjem. [36]

Korištenjem dinamičkog testiranja tim može provjeriti kritične značajke softvera, ali neke od njih mogu ostati bez ikakve procjene. A također mogu utjecati na funkcioniranje, pouzdanost i izvedbu softverskog proizvoda. Dinamičko testiranje izvodi se kako bi se ispunili različiti aspekti u nastavku:

[36] "Practical Software Testing – Manual Testing Help eBook Version 2.0" – A free ebook from STH in association with Chindam Damodar.

- Provjera radi li aplikacija ili softver tijekom i nakon instalacije aplikacije bez ikakvih pogrešaka.
- Provjera je li učinkovito ponašanje softvera.
- Definiranje dinamičkog ponašanja koda.
- Implementiranje koda za testiranje performansi softverske aplikacije u radnom okruženju tijekom procesa dinamičkog testiranja.
- Osigurava istovremeno slanje softverske aplikacije s potencijalima, potrebama i krajnjim korisnikom.
- Operativna tehnika za mjerenje učinka nekoliko stresova okoline na softversku aplikaciju poput mreže, hardvera

Općenito, dinamičko testiranje slijedi već postavljeni postupak kada je odlučeno o pristupima i izvedbama provedbe ispitivanja, a tim koji ga izvodi može krenuti u izvršavanje različitih aktivnosti testiranja. Uz pomoć ovog postupka, tim može pronaći bilo koju nepravilnost u pristupima i strategijama i pomoći da se prikažu svi koraci testiranja. U STLC-u postupak dinamičkog ispitivanja uključuje različite funkcije. I sve se funkcije u procesu dinamičkog ispitivanja oslanjaju na zaključak ranijeg zadatka u procesu testiranja.

Postupak dinamičkog ispitivanja izvršava se u nekoliko koraka. Prvi korak je **specifikacija dizajna**, gdje će timovi dizajnirati test slučajeve. Ovdje stvaramo one test slučajeve koji ovise o zahtjevima i opsegu testiranja utvrđenim prije početka projekta. U ovom koraku možemo odrediti uvjete ispitivanja, dobiti test slučajeve, izdvojiti stavke pokrića i identificirati one značajke koje treba testirati. Druga faza odnosi se na **postavljanje okruženja**. U fazi testnog okruženja pobrinut ćemo se da testno okruženje uvijek bude paralelno proizvodnom okruženju jer se testiranje provodi izravno na softverskom proizvodu. U ovom je koraku glavni cilj dinamičnog ispitivanja instaliranje testnog okruženja, što nam pomaže da uspijemo u testnim strojevima. Nakon toga slijedi treći korak i **izvršenje testa**. Nakon što uspješno instaliramo testno okruženje, izvršit ćemo one test slučajeve pripremljene u primarnoj fazi procesa dinamičkog testiranja. **Analiza i procjena** izvršava se u 4.koraku. Nakon izvršavanja testnih slučajeva, analizirat ćemo i procijeniti ishode

koji su izašli iz testiranja. I usporedit ćemo te ishode s očekivanim rezultatima. Ako očekivani i stvarni rezultati nisu isti prema izvršenju, mi ćemo te testne slučajeve smatrati neuspješnima i prijaviti Bug (grešku) u spremište bugova. **Izvještavanje o greškama** je zadnji korak. Nakon analize testnih slučajeva, bit će prijavljene i zabilježene sve pogreške ili nedostaci između stvarnog rezultata i očekivanog rezultata dotičnoj osobi. Dotična osoba pobrinut će se da je problem riješen i da li pruža kvalitetan proizvod.[37]

Dinamičko testiranje podijeljeno je u dva različita pristupa ispitivanja (Slika 14.), a to su:

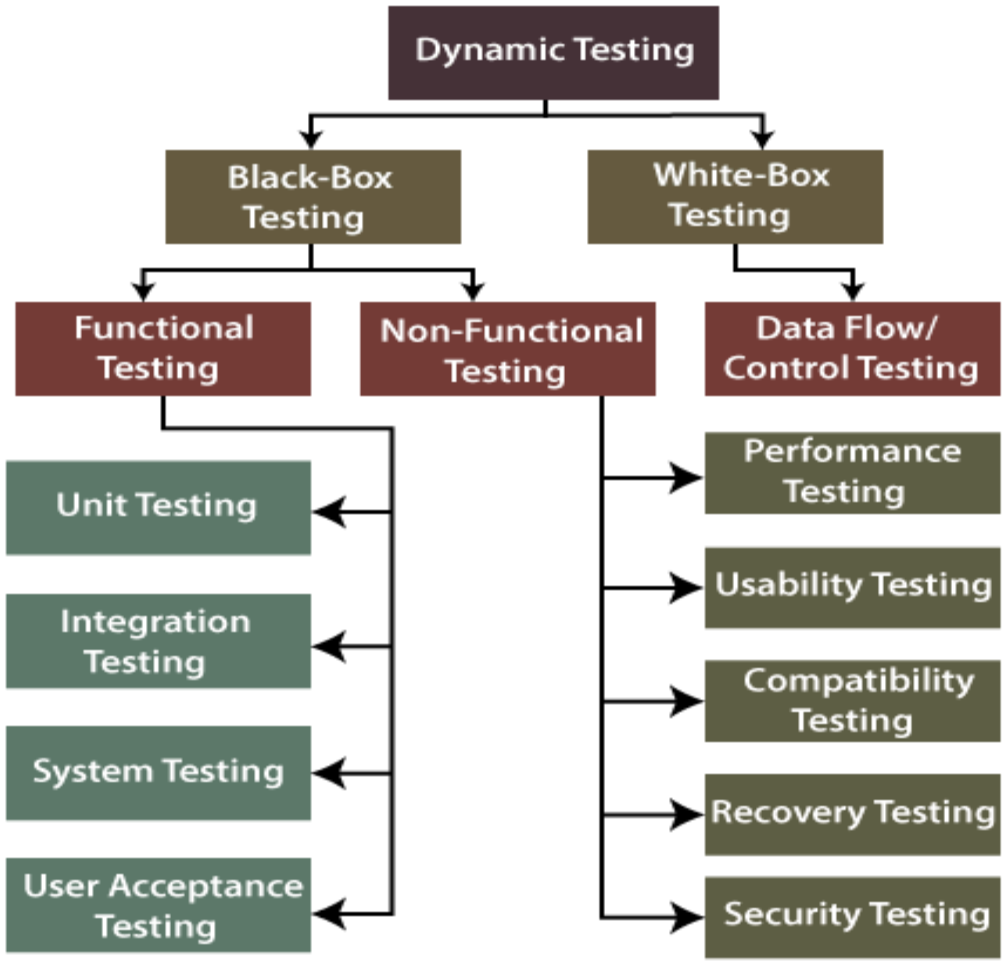
- Testiranje bijele kutije (engl. White box testing)
- Testiranje crne kutije (engl. Black box testing)

Obje tehnike testiranja pomoći će nam da učinkovito izvršimo postupak dinamičkog testiranja jer igraju važnu ulogu u provjeri performansi i kvalitete softvera.

Testiranje bijele kutije

Programeri će izvršiti testiranje bijele kutije, gdje će testirati svaki redak programskog koda. Kada programeri izvrše testiranje bijele kutije, a zatim pošalju softversku aplikaciju timu za testiranje, testni tim će izvršiti testiranje crne kutije, potvrditi aplikaciju kao i zahtjeve. Ispitivanje bijele kutije dalje se dijeli na testiranje protoka podataka / kontrolu. Testiranje protoka podataka koristi se za utvrđivanje putova ispitivanja programa prema postavkama opisa i korištenju varijabli u programu. I to se ne odnosi na dijagrame toka podataka.

[37] "Practical Software Testing – Manual Testing Help eBook Version 2.0" – A free ebook from STH in association with Chindam Damodar.



Slika 14. Diagram koji prikazuje dinamičko testiranje

Testiranje crne kutije

Testiranje crne kutije je tehnika ispitivanja gdje inženjer za ispitivanje odabire modul i daje ulaznu vrijednost kako bi promatrao njegovu funkcionalnost i analizu daje li funkcija očekivani izlaz ili ne. Ako je funkcija dala ispravan izlaz, tada će određena funkcija biti označena kao ispravna. Da bi izvršio testiranje crne kutije, inženjer testa trebao bi imati posebno znanje o zahtjevima softvera, a ne programsko znanje o softveru.

Ispitivanje crne kutije dalje se klasificira u dvije vrste, a to su:

- Funkcionalno ispitivanje

- Ispitivanje nefunkcionalnosti

Funkcionalno ispitivanje jedan je od najvažnijih dijelova testiranja crne kutije. Uglavnom se fokusira na specifikaciju aplikacije, a ne na stvarni kod, a inženjer testa testirat će program, a ne sustav. Funkcionalno testiranje koristi se za provjeru funkcionalnosti softverske aplikacije, radi li funkcija prema specifikaciji zahtjeva. U funkcionalnom ispitivanju, svaki je modul testiran davanjem vrijednosti, određivanjem rezultata i provjerom stvarnog rezultata s očekivanom vrijednošću.[38]

Funkcionalno ispitivanje klasificirano je u četiri različite vrste ispitivanja, a to su:

1. Jedinstveno ispitivanje
2. Integracijsko ispitivanje
3. Ispitivanje sustava
4. Ispitivanje prihvaćanja korisnika

Prednosti dinamičkog ispitivanja:

- Ovjerava izvedbu softverske aplikacije.
- Korištenje dinamičkog testiranja osigurava pouzdanost i postojanost softverskog proizvoda.
- Može automatizirati uz pomoć alata koji otkrivaju problematične i složene pogreške u procesu testiranja, a koje se ne mogu pokriti statičkom analizom.
- Pomaže ispitnom timu da prepozna slaba područja okruženja za vrijeme izvođenja.
- Najvažnija prednost upotrebe dinamičkog testiranja u odnosu na statičko testiranje je relativno veći broj programskih pogrešaka.
- U usporedbi sa statičkim ispitivanjem, dinamičko ispitivanje zahtijeva manji broj sastanaka na razini planiranja ispitivanja.
- Primjenjuje softver od kraja do kraja i isporučuje softver bez grešaka.
- Postaje osnovni alat za prepoznavanje svih sigurnosnih prijetnji.

[38] Lonetti F., Marchetti E.; "Emerging Software Testing Technologies" Advances in Computers, pp. 91–143. New York: Elsevier, 2018

- U dinamičkom testiranju možemo otkriti problematične bugove koji su možda izbjegli procese pregleda.
- Također identificira one greške koje se statičkim ispitivanjem ne mogu primjetiti.
- Dinamičko testiranje također može pronaći sigurnosne prijetnje, koje osiguravaju bolju i sigurniju aplikaciju.

5.3 Fuzz testiranje

Fuzz testiranje ili zamagljivanje je dinamična tehnika softverskog testiranja pri čemu dolazi do umetanja nevaljanih ili slučajnih podataka zvanih FUZZ u softverski sustav radi otkrivanja pogrešaka u kodiranju i sigurnosnih rupa. Svrha fuzz testiranja je umetanje podataka pomoću automatiziranih ili poluautomatiziranih tehnika i testiranje sustava na razne iznimke poput pada sustava ili kvara ugrađenog koda itd. Fuzzeri ponavljaju ovaj postupak i nadgledaju razvoj događaja dok ne otkriju ranjivost.

Fuzz testiranje izvorno je razvio Barton Miller na Sveučilištu Wisconsin 1989-te godine. Odnedavno se fuzz testiranje primjenjuje na sigurnosnim protokolima klijent-poslužitelj i virtualnim strojevima, kao i na definiciji novog kriterija pokrivenosti. Iako su se prva fuzz testiranja pristupa isključivo temeljila na slučajno generiranim testnim podacima (engl. random fuzzing), napredak u simboličkim proračunima, testiranje temeljeno na modelu, kao i dinamičko generiranje testnih slučajeva doveli su do naprednijih tehnika fuzzinga poput fuziranja temeljenog na mutacijama, nejasno generiranje ili nejasno sivo polje. [39]

Primjena Fuzz testiranja na sigurnosne protokole i virtualne strojeve temelji se na istom, uobičajeno prihvaćenom pristupu visoke razine: sakupljajte valjane ulaze i mutirajte ih da biste dobili nove ulaze. Doprinosi su ograničeni na određenu strategiju koja se koristi za mutiranje unosa. U slučaju sigurnosnih protokola klijent-poslužitelj, testiranje fuzz-a provedeno je hvatanjem i mutiranjem poruka koje su razmijenjene između klijenta i poslužitelja.

[39] Sutton M., Greene A., Amini P.; “Fuzzing: Brute Force Vulnerability”, Discovery 1st Edition, Kindle Edition, 2007.

Slučajan fuzzing (engl. Random fuzzing) je najjednostavnija i najstarija fuzz tehnika ispitivanja. Tok slučajnih ulaznih podataka se, u scenariju crnog okvira, šalje u program koji se ispituje. Ulazni podaci mogu se npr. slati kao opcije naredbenog retka, događaji ili paketi protokola. Ova vrsta fuzzinga posebno je korisna za testiranje reakcije programa na velike ili nevaljane ulazne podatke. Iako slučajno zamagljivanje može pronaći već ozbiljne ranjivosti, moderan fuzzing ima detaljno razumijevanje ulaznog formata koji očekuje program koji se testira.

Fuzzing temeljen na mutacijama je vrsta fuzziranja kod koje fuzzer ima određeno znanje o ulaznom formatu programa koji se ispituje, te na temelju postojećih uzoraka podataka, fuzzi alati temeljeni na mutacijama generiraju nove podatke (mutante), na temelju heuristike, koje koristi za fuzziranje. Dostupan je širok raspon fuzzing pristupa temeljenih na mutacijama za različite domene.

Fuzziranje temeljeno na generiranju koristi model (ulaznih podataka ili ranjivosti) za generiranje testnih podataka iz ovog modela ili specifikacije. U usporedbi s čistim slučajnim fuzzingom, fuziranjem zasnovanim na generiranju obično se postiže veća pokrivenost testiranim programom, posebno ako je očekivani format unosa prilično složen. [40]

Napredne tehnike fuzzinga kombiniraju nekoliko prethodno spomenutih pristupa, npr. koriste kombinaciju tehnika temeljenih na mutacijama i generiranju, kao i promatranje programa koji se testira i ta opažanja koriste za konstruiranje novih podataka o ispitivanju. To pretvara fuzziranje u **tehniku testiranja sive kutije** koja također koristi simboličke proračune koji se obično shvaćaju kao tehnika koja se koristi za statičku analizu programa.

Mnoge organizacije prihvaćaju I uključuju fuzziranje u svoje standardne razvojne procese iz nekoliko razloga:

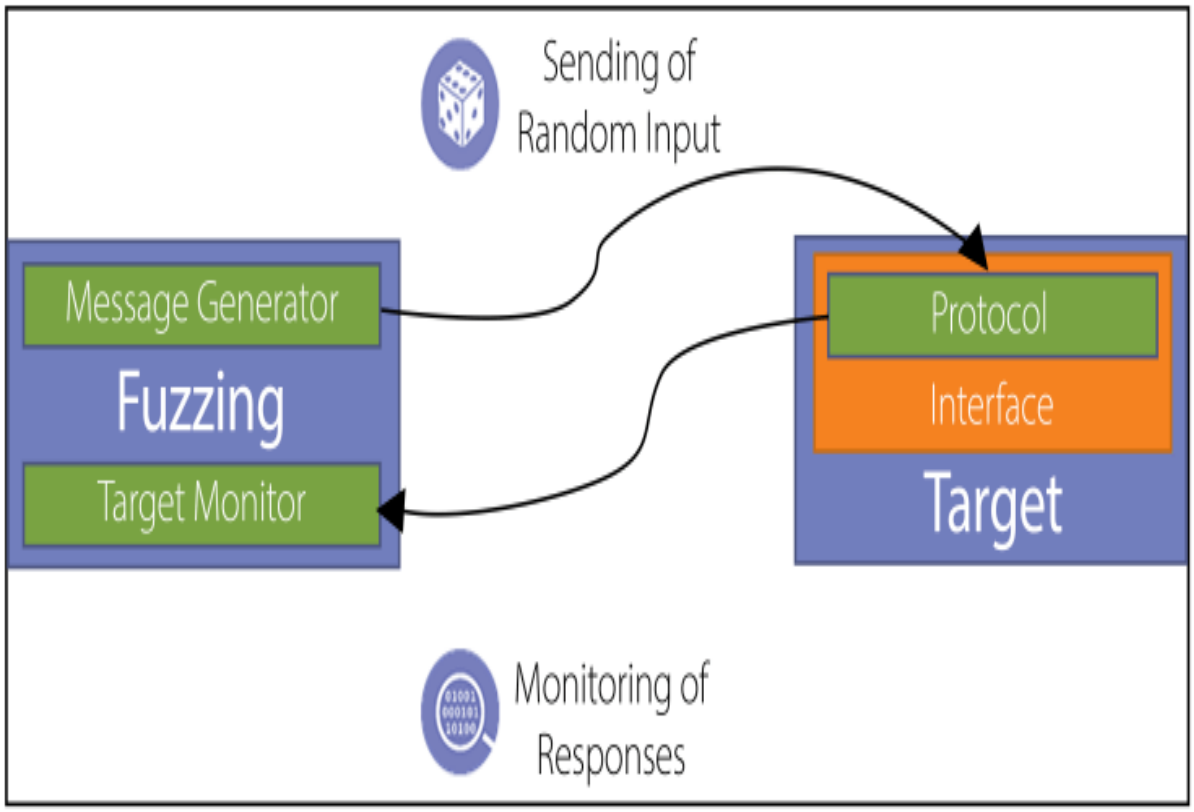
1. Fuzzing ne identificira samo problem, on također pokazuje uzrok problema i kako napadač može komunicirati s njim u stvarnom napadu.
2. Fuzzing dokazuje da postoji ranjivost, identificirajući probleme bez lažnih pozitivnih rezultata.

[40] Sutton M., Greene A., Amini P.; "Fuzzing: Brute Force Vulnerability", Discovery 1st Edition, Kindle Edition, 2007.

3. Fuzzing je potpuno automatiziran i može se samostalno izvoditi danima ili čak tjednima, identificirajući sve više i više ranjivosti u sustavu koji se ispituje.
4. Fuzzing je vrlo koristan za programere. Uloga programera je razviti i poboljšati značajke proizvoda. Iako tradicionalni sigurnosni alati samo ukazuju na nedostatke, fuzzeri pokazuju rezultat nedostatka i pokazuju učinak njegova rješavanja.

Način provedbe fuzzing testiranja:

1. Generiranje test slučajeva
2. Povezivanje s ciljem s ciljem isporuke podataka za unos
3. Nadgledanje sustava za otkrivanje padova, grešaka sustava



Slika 14. Funkcioniranje fuzzinga

Prvo se **generiraju test slučajevi**. Svaki slučaj sigurnosnog testa može se generirati kao slučajni ili polu-slučajni skup podataka, a zatim poslati kao ulaz u aplikaciju. Skup podataka može se generirati u skladu sa zahtjevima formata koji nalaže sustav ili kao potpuno neispravni dio podataka koji sustav nije trebao razumjeti ili obraditi. Generiranje testnih slučajeva razlikovat će se ovisno o tome koristi li se fuzziranje na temelju mutacije ili generacije. Neovisno o tome, bit će nešto što treba nasumično transformirati, bilo da se radi o polju određene vrste ili proizvoljnom dijelu podataka.

Povezivanje s ciljnim programom radi pružanja nejasnih podataka često je jednostavno. Za mrežne protokole može uključivati slanje testnog slučaja mrežom ili odgovaranje na zahtjev klijenta. Za formate datoteka to bi moglo značiti izvršavanje programa s argumentom naredbenog retka koji pokazuje na testni slučaj. Međutim, ponekad se ulaz pruža u obliku koji nije trivijalno generirati na automatiziran način ili gdje skriptiranje programa za izvršavanje svakog test slučaja ima velike troškove i pokazuje se vrlo sporim. Kreativno razmišljanje u tim slučajevima može otkriti načine vježbanja odgovarajućeg dijela koda s pravim podacima. [41]

Otkrivanje grešaka od primarne je važnosti za fuzziranje. Ako ne možete točno odrediti kada se program srušio, nećete moći prepoznati testni slučaj kao pokretač programske pogreške. Postoji niz uobičajenih načina da se tome pristupi:

- Program za ispravljanje pogrešaka - pruža najtočnije rezultate, a program za ispravljanje pogrešaka možete skriptirati tako da vam pruži trag rušenja čim se otkrije rušenje. Međutim, priključivanje programa za uklanjanje pogrešaka može znatno usporiti programe i može uzrokovati prilično velike troškove. Što manje testnih slučajeva možete generirati u određenom vremenskom razdoblju, to ćete imati manje šansi da pronađete pad.
- Praćenje nestaje li postupak - Umjesto prilaganja programa za ispravljanje pogrešaka, jednostavno vidjeti postoji li ID cilja još uvijek na sustavu nakon izvršavanja testnog slučaja. Ako je postupak nestao, vjerojatno se srušio. Kasnije možete ponovno pokrenuti testni slučaj u programu za otklanjanje pogrešaka ako

[41] Sutton M., Greene A., Amini P.; "Fuzzing: Brute Force Vulnerability", Discovery 1st Edition, Kindle Edition, 2007.

želite dodatne informacije o padu. To možete čak i učiniti automatski za svaki pad, istodobno izbjegavajući usporavanje postavljanja programa za ispravljanje pogrešaka za svaki slučaj.

- "Timeout" - Ako program normalno reagira na testne slučajeve, postaviti vremensko ograničenje nakon kojeg pretpostavljate da se program srušio ili zamrznuo. To također može otkriti greške zbog kojih program ne reagira, ali ne mora se i prekinuti.

Prednosti Fuzz testiranja:

- Fuzz testiranje poboljšava testiranje sigurnosti softvera.
- Greške pronađene u fuzingu ponekad su ozbiljne i većinu vremena ih koriste hakeri, uključujući padove, curenje memorije, neobrađenu iznimku itd.
- Ako testeri ne uspiju primijetiti bilo koju programsku pogrešku zbog ograničenja vremena i resursa, one će se također naći u Fuzz testiranju.

Nedostaci fuzz testiranja:

- Fuzz testiranje samo po sebi ne može pružiti cjelovitu sliku opće sigurnosne prijetnje ili grešaka.
- Fuzz testiranje je manje učinkovito za rješavanje sigurnosnih prijetnji koje ne uzrokuju pad programa, poput nekih virusa, crva, trojanaca itd.
- Fuzz testiranje može otkriti samo jednostavne greške ili prijetnje.
- Za učinkovito obavljanje treba značajno vrijeme.
- Postavljanje graničnog uvjeta sa slučajnim ulazima vrlo je problematično, ali sada upotreba deterministčkih algoritama temeljenih na korisničkim ulazima većina testera rješava ovaj problem.

5.4 Test prodora

Testiranje prodiranja (poznato i kao testiranje olovke ili etičko hakiranje) sustavni je postupak ispitivanja ranjivosti u mrežama i aplikacijama. Za razliku od fuzzing-a koji koristi slučajne ili nevaljane podatke za testiranje sustava, test prodora koristi poznate cyber-napade ili ranjivosti za pokretanje simuliranih napada, identificiranje potencijalnih ranjivosti i odabir protumjera za ublažavanje tih ranjivosti. Shvatite to kao navođenje nekoga da se ponaša poput lopova automobila kako bi pokušao provaliti u vaš automobil i dobiti pristup, kroz ovaj "trik" proizvođač može naučiti puno o tome kako može bolje osigurati pristupne sustave svog vozila. [42]

To je u osnovi kontrolirani oblik hakiranja - 'napadači' djeluju u ime korisnika kako bi pronašli i testirali slabosti koje bi kriminalci mogli iskoristiti, kao što su:

- Neadekvatna ili nepravilna konfiguracija.
- Poznate i nepoznate hardverske ili softverske pogreške.
- Operativne slabosti u procesima ili tehničke protumjere.

Iskusni ispitivači prodora oponašaju tehnike koje koriste kriminalci bez nanošenja štete. To vam omogućuje otklanjanje sigurnosnih nedostataka zbog kojih je vaša organizacija ranjiva.

Nove ranjivosti u internetskoj sigurnosti otkrivaju se - i iskorištavaju ih kriminalci - svaki tjedan. Proaktivno identificiranje ključno je za sigurnost. Samo test prodora koji provodi obučeni sigurnosni stručnjak može vam dati pravilno razumijevanje sigurnosnih problema s kojima se suočavate.

Da bismo se zaštitili, trebali bismo redovito provoditi testove penetracije kako bismo:

[42] Liu C., More J., Stieber A. J.; “Breaking into Information Security: Crafting a Custom Career Path to Get the Job You Really Want”; Elsevier, 2016.

- Utvrdili sigurnosne nedostatke kako bi ih mogli riješiti ili primijeniti odgovarajuće kontrole.
- Osigurali da su postojeće sigurnosne kontrole učinkovite.
- Testirali novi softver i sustave na bugove.
- Otkrili nove greške u postojećem softveru.
- Podržali usklađenost svoje organizacije s EU GDPR (Opća uredba o zaštiti podataka) i DPA (Zakon o zaštiti podataka) 2018, te ostalim relevantnim zakonima ili propisima o privatnosti.
- Omogućili svoju usklađenost sa standardima kao što je PCI DSS (Standard zaštite podataka industrije platnih kartica).
- Uvjerili kupce i ostale dionike da su njihovi podaci zaštićeni.

Faze penetracijskog prodiranja:

1. Prikupljanje informacija
2. Mapiranje mreže
3. Identificiranje ranjivosti
4. Penetracija
5. Dobivanje pristupa i povećanje ovlasti
6. Daljnje popisivanje objekata
7. Kompromitacija sustava
8. Održavanje pristupa i skrivanje tragova

Prije nego što test olovke započne, testeri i njihovi klijenti moraju se uskladiti s ciljevima testa, tako da je opsežno i pravilno izveden. Morat će znati koje vrste testova trebaju izvoditi, tko će biti svjestan da je test pokrenut, s koliko informacija i pristupa testera moraju započeti te druge važne detalje koji će osigurati da test bude uspjeh.

Prikupljanje informacija je postupak koji uključuje korištenje Interneta za pronalazak informacija o ciljnom sustavu, organizaciji ili osobi, uz pomoć tehničkih (DNS/WHOIS) i netehničkih metoda (pretraživači, novinske grupe, liste elektroničke pošte i sl.). Kod provođenja bilo kakvog testa na informacijskom sustavu, prikupljanje informacija je ključno i osigurava potrebne preduvjete za nastavak testiranja. Prilikom prikupljanja podataka, važno je biti što domišljatiji te pokušati istražiti sve moguće putove za lakše razumijevanje ciljnog sustava i njegovih resursa. U ovoj fazi testiranja, korisno je sve do čega se može doći: organizacijske brošure, poslovne kartice, prospekti, novinske reklame, interni papiri i dr.

Specifične mrežne informacije prikupljene u prošloj fazi, koriste se i proširuju prilikom izrade vjerojatne mrežne topologije mete. U fazi **mapiranja mreže** timovi izvode različite vrste izviđanja na svoju metu. S tehničke strane, informacije poput IP adresa mogu pomoći u utvrđivanju informacija o vatrozidima i drugim vezama. S osobne strane, podaci jednostavni poput imena, naslova poslova i adresa e-pošte mogu imati veliku vrijednost. Postupak mapiranja mreže obuhvaća: pronalazak aktivnih računala, pretraživanje priključaka i servisa, određivanje vanjskih rubova mreže (usmjerivača, vatrozida), identifikaciju kritičnih servisa, utvrđivanje informacija o operacijskom sustavu (eng. OS fingerprinting), identifikaciju ruta korištenjem MIB (eng. Management Information Base) baze i utvrđivanje informacija o servisima (eng. Service fingerprinting). [43]

Informirani o svom cilju, testeri prodora mogu se početi pokušavati infiltrirati u okoliš, iskorištavajući sigurnosne slabosti i pokazujući koliko duboko mogu ući u mrežu. Prilikom **identifikacije ranjivosti**, analizator detektira slabe točke sustava koje su pogodne za zloporabu. Aktivnosti kojima se postiže takva detekcija uključuju: identifikaciju ranjivih servisa korištenjem servisnih poruka (eng. banners), pretraživanje ranjivosti s ciljem otkrivanja poznatih nedostataka - informacije vezane uz poznate ranjivosti mogu se pronaći u proizvođačevim sigurnosnim oglasima ili u javnim bazama podataka, kao što su SecurityFocus, Secunia i sl., popisivanje

[43] Weidman G.; "Penetration Testing: A Hands-On Introduction to Hacking"; no stretch press, San Francisco, 2014.

otkrivenih ranjivosti, procjenu očekivanog utjecaja (klasifikacija pronađenih ranjivosti) i identifikaciju putova napada i scenarija za zloporabu.

Analizator pokušava ostvariti neovlašten pristup zaobilaženjem sigurnosnih ograničenja, pri tome nastojeći dobiti što veće ovlasti. Proces **penetracije** može podijeliti u nekoliko faza: pronalazak programskog koda koji iskorištava ciljane ranjivosti (eng. Exploit, razvoj alata/skripti - u nekim okolnostima potrebno je kreirati vlastite alate i skripte za testiranje i za povećanje učinkovitosti, testiranje alata/kôda za dokazivanje koncepta, prilagodba alata/kôda za dokazivanje koncepta, potvrda ili pobijanje postojanja ranjivosti - jedino testiranjem ranjivosti analizatori mogu sa sigurnošću potvrditi ili pobiti postojanje ranjivosti, dokumentacija - mora sadržavati detaljan opis putova zloporabe, utjecaja koji je ostvaren na sustav i dokaza postojanja ranjivosti. [44]

Ukoliko u fazi penetracije nije uspio pokušaj **dobivanja pristupa** ovaj korak nudi neke alternativne mogućnosti. Ako je, ipak, penetracija dala određene rezultate, jednako kao i kad to nije slučaj, ovaj korak omogućuje dodatno **povećanje ovlasti**.

Faza **daljnjeg popisivanja objekata** sastoji od sljedećih koraka: otkrivanja kriptiranih zaporki za probijanje sustava koji nije spojen na mrežu, otkrivanja zaporki (kriptiranih ili otvorenog teksta) korištenjem sniffer alata i drugih tehnika, analize prometa, prikupljanja kolačića (eng. cookie) i njihovog korištenja za iskorištavanje sjednica ili napade na zaporke, prikupljanja adresa elektroničke pošte, identifikacije ruta i mreža, i mapiranja internih mreža i ponovnog izvođenja prethodnih koraka, sa sustavom u danom stanju kao polaznom točkom. [45]

Jedna ranjivost u sustavu dovoljna je za izlaganje čitave mreže, neovisno o tome koliko je sigurna njena periferija. Svaki je sustav jak (u ovom slučaju siguran) onoliko, koliko su jaki njegovi najslabiji dijelovi što se otkriva u fazi **kompromitacije sustava**. Komunikacija između udaljenih

[44] Weidman G.; "Penetration Testing: A Hands-On Introduction to Hacking"; no stretch press, San Francisco, 2014.
[45] Liu C., More J., Stieber A. J.; "Breaking into Information Security: Crafting a Custom Career Path to Get the Job You Really Want"; Elsevier, 2016.

korisnika/podružnica i organizacijskih mreža može se zaštititi autentikacijom i enkripcijom, korištenjem tehnologija kao što je VPN (eng. Virtual Private Network), kako bi se osigurala autentičnost i privatnost prenošenih podataka. Međutim, to ne jamči pouzdanost krajnjih točaka u komunikaciji.

Održavanje pristupa i skrivanje tragova nezaobilazan su dio penetracijskog testiranja, a analizatoru osiguravaju stalnu i trajnu prisutnost na kompromitiranom sustavu bez mogućnosti razotkrivanja.

Postojeći standardi penetracijskog testiranja

Ljudi su često iznenađeni kada uvide mogućnost postojanja strukture i organizacije u procesu penetracijskog testiranja. Unatoč tome, postoji nekoliko izvora koji standardiziraju ovaj proces.

Priručnik za metodologiju sigurnosnog ispitivanja otvorenog koda

OSSTMM (engl. Open Source Security Testing Methodology Manual) je priručnik koji detaljno opisuje proces penetracijskog testiranja. Cilj priručnika, koji su njegovi autori postavili još za vrijeme njegovog sastavljanja, je definiranje stroge metodologije penetracijskog testiranja, pri čemu se moraju zadovoljiti tri uvjeta:

- Konzistencija
- Ponovljivost
- Pouzdanost rezultata

OSSTMM je u svojoj srži skup uputa kojima je cilj provođenje iscrpnih penetracijskih testova koji će pokriti sva potrebna područja, pritom pazeći na pridržavanje zakonskih odredbi. Rezultat testiranja učinjenog prema ovom standardu kvantificira stupanj opasnosti, konzistentan je i mora biti ograničen na prezentaciju pronađenih činjenica. Sam priručnik podijeljen je u šest dijelova (eng. channels):

- Informacijska sigurnost

- Sigurnost procesa
- Sigurnost Internet tehnologija
- Sigurnost komunikacija,
- Sigurnost bežičnih tehnologija
- Fizička sigurnost

National Institute of Standards and Technology (NIST) standard

Nacionalni institut znanosti i tehnologije Sjedinjenih Američkih Država (eng. National Institute of Science and Technology - NIST) načinio je dokument s naslovom Special Publication 800-42, Guideline on Network Security Testing. Cilj dokumenta je sistematično propisivanje elemenata testiranja sigurnosti u državnim organizacijama SAD-a. On identificira preduvjete koje je potrebno ispuniti za početak testiranja i preporuča prioritete kojima je moguće testiranje provesti i s ograničenim resursima. Također doprinosi izbjegavanju dvostrukog napora pružajući sustavan pristup cijeloj problematici.

Dodatna mu je prednost i postojanje više razina testiranja koje, ovisno o organizaciji nad kojom se postupak primjenjuje, mogu dovesti do značajne uštede sredstava. Temeljni naglasak dokumenta stavljen je na pružanje osnovnih informacija o alatima i tehnikama koje stoje na raspolaganju osobi koja želi započeti postupak testiranja sigurnosti.

Okvir za procjenu sigurnosti informacijskih sustava

ISSAF (engl. Information Systems Security Assessment Framework) je strukturirani radni okvir koji područje procjene sigurnosti računalnog sustava organizira u različite domene. Osim toga, on detaljno opisuje sasvim specifične testove koji se provode u svakoj od njih. Iako uključuje vrlo opsežan skup sigurnosnih procedura, još se uvijek smatra standardom u razvoju, te se nije preporučljivo pouzdati u rezultate njegovog provođenja. Također možemo još spomenuti i **OWASP** (Otvoreni projekt sigurnosti web aplikacija), PTF (Okvir za ispitivanje prodora), te PCI DSS (Standard zaštite podataka industrije platnih kartica).

6. Zaključak

Autonomna vozila koriste sustave umjetne inteligencije koji koriste tehnike strojnog učenja za prikupljanje, analizu i prijenos podataka kako bi donijeli odluke koje u konvencionalnim automobilima donosi čovjek. Ovi sustavi, kao i svi IT sustavi, osjetljivi su na napade koji bi mogli ugroziti pravilan rad vozila. Sustavi umjetne inteligencije autonomnog vozila rade neprestano na prepoznavanju prometnih znakova i oznaka na cesti, otkrivanju vozila, procjeni njihove brzine i planiranju puta koji je pred vama. Osim nenamjernih prijetnji, poput iznenadnih kvarova, ovi su sustavi osjetljivi na namjerne napade koji imaju poseban cilj ometati sustav umjetne inteligencije i poremetiti sigurnosno kritične funkcije.

Kako bi se poboljšala sigurnost umjetne inteligencije u autonomnim vozilima, sustavno provjeravanje modela i podataka umjetne inteligencije bitno je kako bi se osiguralo da se vozilo uvijek ispravno ponaša kada se suoči s neočekivanim situacijama ili zlonamjernim napadima. Druga je preporuka da bi kontinuirano provođenje procjene rizika podržano obavještajnim podacima o prijetnjama moglo omogućiti identifikaciju potencijalnih rizika za umjetne inteligencije i novih prijetnji povezanih s preuzimanjem kontrole and vozilom od strane hakera u autonomnoj vožnji. Odgovarajuće sigurnosne politike umjetne inteligencije i sigurnosna kultura umjetne inteligencije trebali bi upravljati cijelim opskrbnim lancem za automobile.

Automobilska industrija trebala bi prihvatiti pristup dizajna sigurnosti za razvoj i primjenu funkcionalnosti umjetne inteligencije, gdje kibernetička sigurnost postaje središnji element digitalnog dizajna od početka. Konačno, važno je da automobilski sektor poveća svoju razinu pripremljenosti i ojača svoje sposobnosti odgovora na incidente za rješavanje novih pitanja kibernetičke sigurnosti povezanih s umjetnom inteligencijom.

POPIS LITERATURE

[1] Bosnjak, I.; Inteligentni transportni sustavi 1. Sveucilište u Zagrebu, Fakultet prometnih znanosti, Zagreb, 2006.

[2] Aizenberg, I.N.; Aizenberg, N.N. and Vandewalle, J.: Multi-Valued and Universal Binary Neurons: Theory, Learning and Applications. Springer, Boston, 2000,

[3] Ondruša, J.; Kollab, E.; Verta, P.; Šarić, Ž. How Do Autonomous Cars Work? Transp. Res. Procedia 2020, 44, 226–233.

[4] Zanchin, B.C.; Adamshuk, R.; Santos, M.M.; Collazos, K.S. On the instrumentation and classification of autonomous cars. In Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics (SMC), Banff, AB, Canada, 5–8 October 2017; pp. 2631–2636.

[5] Wang, Z.; Wu Y.; Niu, Q. Multi-Sensor Fusion in Automated Driving: A Survey. IEEE Access 2020, 8, 2847–2868.

[6] Sawant, H.; Tan, J.; Yang, Q.; Wang, Q. Using Bluetooth and Sensor Networks for Intelligent Transportation Systems. In Proceedings of the 2004 IEEE Intelligent Transportation Systems Conference (ITSC), Washington, DC, USA, 3–6 October 2004.

[7] Jo, K.; Kim, J.; Kim, D.; Jang, C.; Sunwoo, M. Development of Autonomous Car—Part I: Distributed System Architecture and Development Process. IEEE Trans. Ind. Electron. 2014, 61, 7131–7140.

[8] Jo, K.; Kim, J.; Kim, D.; Jang, C.; Sunwoo, M. Development of Autonomous Car—Part II: A Case Study on the Implementation of an Autonomous Driving System Based on Distributed Architecture. IEEE Trans. Ind. Electron. 2015, 62, 5119–5132.

[9] Li, Y.; Ibanez-Guzman, J. Lidar for Autonomous Driving: The Principles, Challenges, and Trends for Automotive Lidar and Perception Systems. IEEE Signal Process. Mag. 2020, 37, 50–61.

[10] De Silva, V.; Roche, J.; Kondoz, A. Robust fusion of LiDAR and wide-angle camera data for autonomous mobile robots. Sensors 2018, 18, 2730.

[11] Wang, H.; Wang, B.; Liu, B.; Meng, X.; Yang, G. Pedestrian recognition and tracking using 3D LiDAR for autonomous vehicle. Robot. Auton. Syst. 2017, 88, 71–78

[12]] A. Chattopadhyay, K. Y. Lam, Security of autonomous vehicle as a cyber-physical system, in: 2017 7th International Symposium on Embedded Computing and System Design (ISED), 2017, pp. 1–6. doi:10.1109/ISED.2017.8303906.

[13] A. M. Wyglinski, X. Huang, T. Padir, L. Lai, T. R. Eisenbarth, K. Venkatasubramanian, Security of autonomous systems employing embedded computing and sensors, IEEE Micro 33 (1) (2013) 80–86. doi:10.1109/MM.2013.18.

[14] S. Jafarnejad, L. Codeca, W. Bronzi, R. Frank, T. Engel, A car hacking experiment: When connectivity meets vulnerability, in: 2015 IEEE Globecom Workshops (GC Wkshps), 2015, pp. 1–6. doi:10.1109/GLOCOMW.2015.7413993.

[15] S. Parkinson, P. Ward, K. Wilson, J. Miller, Cyber threats facing autonomous and connected vehicles: Future challenges, IEEE Transactions on Intelligent Transportation Systems 18 (11) (2017) 2898–2915. doi:10.1109/TITS.2017.2665968.

[16] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno, et al., Comprehensive experimental analyses of automotive attack surfaces., in: USENIX Security Symposium, San Francisco, 2011, pp. 77–92.

[17] M. H. Eiza, Q. Ni, Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity, IEEE Vehicular Technology Magazine 12 (2) (2017) 45–51. doi:10.1109/MVT.2017.2669348.

[18] N. Deepika, V. V. S. Variyar, Obstacle classification and detection for vision based navigation for autonomous driving, in: 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2017, pp. 2092– 2097. doi:10.1109/ICACCI.2017.8126154

[19] J. S. Albus, “The NIST real-time control system (RCS): an approach to intelligent systems research,” Journal of Experimental & Theoretical Artificial Intelligence, vol. 9, no. 2-3, pp. 157–174, 1997.

[20] N. Muscettola, G. A. Dorais, C. Fry, R. Levinson, and C. Plaunt, “Idea: Planning at the core of autonomous reactive agents,” in NASA Workshop on Planning and Scheduling for Space, 2002.

[21] P. Maes, “Behavior-based artificial intelligence,” in Proceedings of the Fifteenth Annual Meeting of the Cognitive Science Society, pp. 74–83, 1993.

[22] A. Brunetti, D. Buongiorno, G. Trotta, V. Bevilacqua: Computer vision and deep learning techniques for pedestrian detection and tracking: a survey Neurocomputing, 300 (2018)

[23] Study by Autonomous Driving, Think ACT, Ronald Berger Strategy Consultatnts Gmbh, Munchen, 2014.

[24] Maurer, Markus, J. Christian Gerdes; Barbara Lenz; Hermann Winner;: "Autonomous Driving: Technical, Legal and Social Aspects". 1st ed. 2016

[25] J. A. P. Marpaung; M. Sain; H. J. Lee;: "Survey on malware evasion techniques: State of the art and challenges,". Proc. Int. Conf. Adv.Commun. Technol., PyeongChang, Korea, 2012.

[26] Mo, Y.;Garone, E.;Casavola, A.; Sinopoli, B.: "False data injection attacks against state estimation in wireless sensor networks". Decision and Control (CDC), 2010 49th IEEE Conference. Siječanj 2011.

[27] Jamal Raiyn: "Data and Cyber Security in Autonomous Vehicle Networks ". U: December 2018, Transport and Telecommunication Journal, 12/2018.

[28] S. Parkinson; P. Ward; K. Wilson; J. Miller; - "Cyber threats facing autonomous and connected vehicles: Future challenges". U: IEEE Transactions on Intelligent Transportation Systems, 11/2017. Str. 2898 – 2915

[29] M. H. Eiza; Q. Ni; - Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity. U: IEEE Vehicular Technology Magazine, 6/2017.

[30] Amara Dinesh Kumar; Koti Naga Renu Chebrolu; Vinayakumar R; Soman KP: A Brief Survey on Autonomous Vehicle Possible Attacks,Exploits and Vulnerabilities. U: eprint arXiv:1810.04144, Listopad 2018.

[31] Mohammed Ali Hezam Al Junaid1; Syed A. A; Mohd Nazri Mohd Warip; Ku Nurul Fazira Ku Azir; Nurul Hidayah Romli: Classification of Security Attacks in VANET: A Review of Requirements and Perspectives. School of Computer and Communication Engineering University Malaysia Perlis, Malaysia, 2018.

[32] Pattnaik O.; Pattanayak B.; - Performance Analysis of MANET and VANET based on Throughput Parameter. Nalanda Institute of Technology, 2017.

[33] Badis, Hakim; Rachedi, Abderrezak - Modeling and Simulation of Computer Networks and Systems. LIGM - Laboratoire d'Informatique Gaspard-Monge, 2015.

[34] Sutton M., Greene A., Amini P.; "Fuzzing: Brute Force Vulnerability", Discovery 1st Edition, Kindle Edition, 2007.

[34] Liu C., More J., Stieber A. J.; “Breaking into Information Security: Crafting a Custom Career Path to Get the Job You Really Want”; Elsevier, 2016.

[35] Weidman G.; “Penetration Testing: A Hands-On Introduction to Hacking”; no stretch press, San Francisco, 2014.

POPIS ILUSTRACIJA

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj diplomski rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.

Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem također, kako 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 **Računalna sigurnost autonomnih vozila**

na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

Student/ica:

U Zagrebu, 8.9.2021

(potpis)