Centar Informacijske Sigurnosti

Sigurnost automobila

siječanj 2012.

CIS-DOC-2012-01-036

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

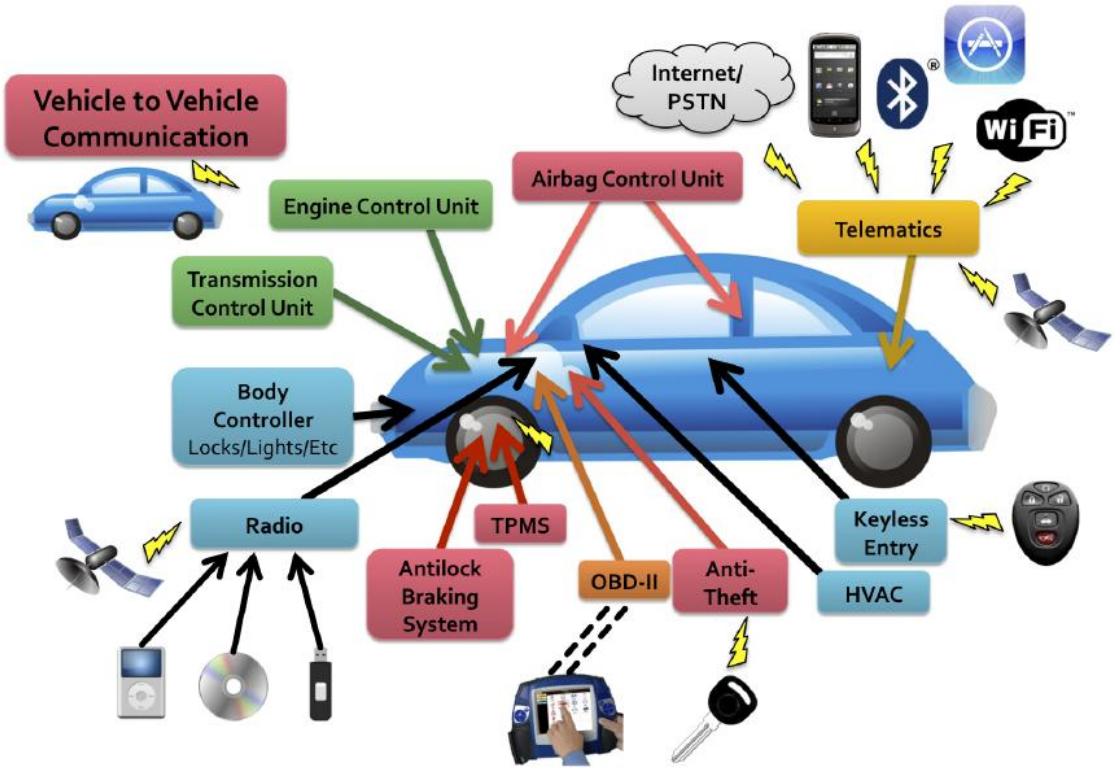
1. Uvod

Ne tako davno, zaštita automobila svodila se na uklanjanje maske (eng. *Compact Disc, DC*) CD svirača (eng. player) ili radija, postavljanje lokota na volan te zaključavanje vrata. Moderni automobili nisu više isključivo mehanički strojevi, oni su u svakom trenutku nadzirani i upravljani desecima digitalnih računala povezanih preko mreže unutar vozila. Ova promjena dovela je do niza poboljšanja u pogledu učinkovitosti i sigurnosti, no s druge strane, sa sobom je donijela i velik broj potencijalnih prijetnji i rizika. Stoga se današnje metode zaštite i osiguravanja automobila sve više približavaju metodama zaštite prijenosnih računala, osobnih računala i poslužitelja. Uvođenje različitih bežičnih mreža kojima se odvija komunikacija između pojedinih dijelova automobila te njihova komunikacija s vanjskim sustavima, unosi dodatne sigurnosne rizike. Da sva razmatranja nisu samo na teoretskoj razini pokazuje i primjer iz ožujka 2010. godine kada je jedan nezadovoljni bivši zaposlenik autocentra u Teksasu iskoristio sustav za udaljenu deaktivaciju automobila kako bi istovremeno ugasio motore više od stotinu udaljenih automobila.

U drugom poglavlju ukratko će biti opisano funkcioniranje modernih automobila sa stajališta tehnoloških inovacija te će kratko biti opisana tri važna elektronička sustava u modernim automobilima. U trećem poglavlju će se provesti analiza modela prijetnje automobilima, s posebnim naglaskom na napadačke površine te na opasnosti koje prijete preko njih i na odgovarajuće postupke zaštite. Kao primjer napada na automobile u praksi opisano je opsežno ispitivanje sigurnosti automobila koje je provela skupina istraživača sa Sveučilišta u Washingtonu i Sveučilišta u Kaliforniji - San Diego. Oni su simulirali različite vrste napada na automobil u mirovanju i u vožnji. Navedeni su i kratko diskutirani rezultati njihovog ispitivanja. Na kraju su dana predviđanja vezana uz budućnosti automobilske sigurnosti.

2. Suvremene tehnologije u modernim automobilima

Na prvi pogled osobni se automobili kroz preko osamdeset godina masovne proizvodnje nisu u svojoj suštini značajno promijenili. I dalje ih pokreće jedan benzinski ili dizelski motor s unutarnjim izgaranjem, voze se na četiri kotača, a njima se upravlja pomoću volana, papučice gasa, kočnice i mjenjača. No u posljednja dva desetljeća, razvojem osobnih računala i računalne tehnologije, unutarnji sustav upravljanja automobilom doživio je drastične promjene. Današnji automobili ispod svoje površine sadrže mnogobrojna računala koja upravljaju i nadziru senzore, različite dijelove automobila te vozača i putnike. Najnovije procjene govore da prosječna luksuzna limuzina sadrži više od 100 MB binarnog koda raspodijeljenog između pedeset do sedamdeset nezavisnih računala - elektroničkih upravljačkih jedinica (eng. *Electronic Control Units, ECUs*), pri čemu su te elektroničke upravljačke jedinice međusobno povezane vrstom mreže kontrolera (eng. *Controller Area Network, CAN*). Takve elektroničke upravljačke jedinice upravljaju svim funkcionalnim dijelovima današnjih automobila; od upravljanja, prijenosa, kočnica i svjetala do sustava grijanja i hlađenja, unutrašnjeg osvjetljenja te CD svirača (Slika 1). Mnoge funkcije zahtijevaju složeno međudjelovanje više različitih elektroničkih upravljačkih jedinica. U nastavku su ukratko opisana tri važna elektronička sustava.



Slika 1. *Shema digitalnih ulazno-izlaznih kanala u modernom automobilu*
Izvor: *Comprehensive Experimental Analyses of Automotive Attack Surfaces*

2.1. Elektronička kontrola stabilnosti

Elektronička kontrola stabilnosti (eng. *Electronic Stability Control, ESC*) je elektronički sustav za poboljšanje dinamičke stabilnosti i upravljivosti automobila koji kočenjem pojedinim kotačima sprečava zanošenje i ispravlja putanju već zanesenog automobila. Drugi naziv za ovaj sustav je ESP (eng. *Electronic Stability Program*). ESP sustavom upravlja pametna elektronika, na temelju informacija koje mjere pripadajući senzori: zakrenutost upravljača, brzina vrtnje svakog kotača, uzdužna i bočna brzina automobila, uzdužno i bočno ubrzanje automobila, te brzina vrtnje automobila oko vertikalne osi. Iz dobivenih se informacija precizno proračunava položaj vozila u odnosu na željenu putanju te se aktivira povremeno kočenje pojedinih kotača.

2.2. Sustav protiv blokiranja kotača

Sustav protiv blokiranja kotača (eng. *Anti-lock Braking System, ABS*) sprečava blokiranje kotača pri kočenju punom snagom ili na skliskom kolniku. Blokiranjem kotača pri kočenju znatno se smanjuje koeficijent trenja, posebice u poprečnom smjeru. Zbog toga se produžuje zaustavni put, a automobil postaje potpuno neupravljiv. Kako se to ne bi dogodilo, ABS upravljačka jedinica pomoću senzora broja okretaja kotača nadzire broj okretaja svih kotača vozila. Ako neki od njih zaprijeti blokiranjem, magnetni ventil u upravljačkoj jedinici sustava protiv blokiranja kotača smanjuje tlak kočenja za odgovarajući kotač sve dok se on ponovno ne počne slobodno okretati. Nakon toga se tlak iznova povećava do granice blokiranja. Zahvaljujući ovom sustavu, vozilo ostaje stabilno i njime se može upravljati.

2.3. Adaptivni tempomat

Adaptivni tempomat (eng. *Adaptive Cruise Control, ACC*) je automatski uređaj za podešavanje udaljenosti od vozila ispred, koji neprekidno mjeri udaljenost među vozilima te po potrebi ubrzava ili usporava automobil. Sustav adaptivnog tempomata se nadograđuje na sustav tempomata koji elektroničkim nadzorom održava brzinu automobila. Središte sustava je upravljačka elektronika s radarskim osjetnikom udaljenosti. Smješten je u prednjem dijelu vozila (masci ili reflektorima). Radi na osnovi Dopplerovog efekta[1] mjereći relativnu brzinu u odnosu na automobil ispred te u ovisnosti o izmjerenoj brzini ispravlja brzinu vozila kako bi postojao sigurnosni razmak među vozilima. Opširniji opisi ovih sustava, kao i brojnih drugih koji su prisutni u modernima automobilima, mogu se pronaći na poveznici [7].

3. Modeli prijetnje automobilima

Pri definiranju modela prijetnje važno je razlikovati:

- **tehničke mogućnosti** - opisuju protivnikova znanja o vozilima na koja je usmjeren njegov napad kao i njegove sposobnosti analize sustava u svrhu razvoja zlonamjernog koda za različite ulazno-izlazne kanale,
- **operacijske mogućnosti** - opisuju protivnikove zahtjeve za dostavljanjem zlonamjernog koda do određenih ulaznih dijelova sustava.

Operacijske mogućnosti ugrubo se dijele na tri kategorije:

- **neizravan fizički pristup**,
- **bežični pristup kratkog dometa**,
- **bežični pristup velikog dometa**.

U nastavku je pobliže opisana svaka od ovih kategorija.

3.1. Neizravni fizički pristup

Današnji automobili osiguravaju nekoliko fizičkih sučelja koja bilo izravno, bilo neizravno pristupaju mrežama unutar automobila. Pod pojmom fizičke napadačke površine podrazumijevamo upravo ovaj način pristupa, uz ograničenje da protivnik ne mora nužno izravno pristupiti postojećim fizičkim sučeljima, već im može pristupiti i posredno.

Priključak OBD-II (eng. *On Board Diagnostics*) predstavlja najznačajnije automobilsko sučelje koje osigurava izravan pristup CAN (eng. *Controller Area Network*) sabirnici automobila i omogućuje dovoljan pristup kako bi se ugrozio velik broj automobilskih sustava. Navedeni priključak koristi se za povezivanje automobila s prijenosnim računalom najčešće u svrhu dijagnostike i servisa.

[1] **Dopplerov efekt** je promjena promatrane valne duljine vala zbog međusobnog približavanja ili udaljavanja izvora i promatrača. Jedna od značajnih primjena mu je u policijskim prometnim radarima za određivanje brzine kojom se vozilo kreće.

Druga važna skupina fizičkih sučelja usmjerena je na sustave za zabavu. Gotovo svi današnji automobili sadrže CD svirač koji omogućuje reprodukciju različitih audio formata. Sve je češća pojava priključaka USB (eng. *Universal Serial Bus*) i iPod kojima se omogućuje korisnički nadzor nad medijskim sustavom automobila. Protivnik može iskoristiti upravo ova sučelja kako bi zlonamjerni kod ubacio na CD zajedno s podacima ili kao glazbenu datoteku. Promatrajući CD player kao izdvojenu jedinicu ovaj slučaj ne predstavlja značajnu prijetnju, no kako su različiti sustavi u automobilu povezani sabirnicama jedna ugrožena komponenta može poslužiti kao vrata za napad na ostale komponente.

3.2. Bežični pristup kratkog dometa

Neizravni fizički pristup ima brojne nedostatke, koji uključuju operacijsku složenost, zahtjevnost kod preciznog ciljanja napada te nemogućnost upravljanja vremena napada. U bežični pristup kratkog dometa spadaju napadačke površine za automobilska bežična sučelja sa slabijim operacijskim zahtjevima za napadača. Bežični pristup kratkog dometa uključuje:

- Bluetooth, koji je gotovo postao standard poziva slobodnih ruku u automobilima; u automobilima se koriste Bluetooth uređaji s dosegom od 10 metara,
- daljinsko otključavanje (eng. *Remote Keyless Entry*), koje je uključeno u gotovo sve moderne automobile, omogućuje i neke dodatne opcije poput pokretanja motora,
- radiofrekvencijske identifikacijske ključeve (eng. *Radio Frequency Identification keys, RFID keys*), koji onemogućuju korištenje automobila bez odgovarajućeg ključa,
- sustav nadziranja tlaka u gumama (eng. *Tire Pressure Monitoring System, TPMS*), koji obavještava vozača o premalom ili prevelikom tlaku u gumama,
- WiFi (eng. *wireless fidelity*), koji općenito označava bežičnu razmjenu podataka preko računalne mreže,
- usmjerene komunikacije kratkog dometa (eng. *Dedicated Short-Range Communications, DSRC*), koje su tek u razvoju, a njihova namjena bi bila komunikacija između vozila s ciljem zaobilaženja gužvi i ublažavanja posljedica nesreća.

Za ovu skupinu napadačkih površina pretpostavljamo da protivnik može postaviti bežični odašiljač u blizini automobilskog prijemnika (između 5 i 300 metara, ovisno o kanalu).

3.3. Bežični pristup velikog dometa

Digitalni pristupni kanali velikog dometa dijele se u dvije kategorije:

- **razašiljački kanali** (eng. *broadcast channels*) - to su kanali koji nisu izravno usmjereni prema automobilu, no moguće ih je uključiti prijamnicima na zahtjev,
- **adresabilni kanali** (eng. *addressable channels*) - prestavljaju važnu skupinu kanala zbog ugroženosti napadima i dostupnosti potencijalnim napadačima.

Moderni automobil sadrži razne višeodredišne prijamnike za signale velikog dosega:

- GPS (eng. *Global Positioning System*), služi za navigaciju,
- satelitski radio,
- digitalni radio,
- sustav radio podataka (eng. *Radio Data System, RDS*) predstavlja uslugu koju daju radiopostaje, pored programa koji se čuje odašilju se i dodatne informacije u obliku šifriranih digitalnih signala, koje mogu analizirati radiouređaji prikladni za RDS,
- kanal poruka o prometu (eng. *Traffic Message Channel, TMC*), omogućuje dinamičko vođenje prema odredištu, kod kojega navigacijski sustav samostalno prepoznaje zastoje u prometu i nudi alternativne pravce.

Vjerojatno najvažniji dio bežične napadačke površine velikog dosega jest izloženost udaljenim telematičkim sustavima[2] koji osiguravaju stalnu povezanost preko govornih ćelija i podatkovnih

[2] Telematički sustav detaljnije je opisan u poglavlju 3.4.1. Telematički sustav

mreža. Ovakvi ćelijski kanali pružaju mnoge prednosti za napadače: može im se pritupiti s proizvoljne udaljenosti i na razne anonimne načine, najčešće imaju ralativno veliku širinu pojasa te su pojedinačno adresabilni.

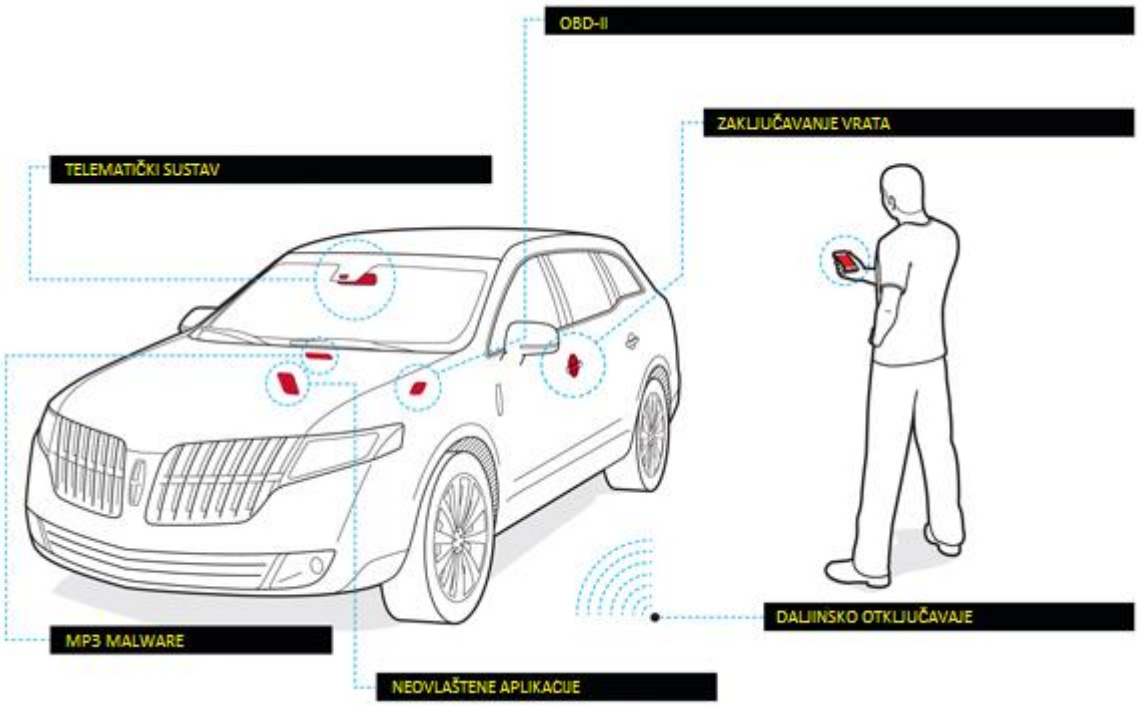
3.4. Napadačke površine i zaštita

Kod napada na automobile napadači pokušavaju preko nekih kritičnih dijelova sustava zadobiti određeni nadzor nad sustavom i nanijeti mu štetu. Takvi kritični dijelovi nazivaju se napadačke površine.

Neke od najvažnijih napadačkih površina (Slika 2) kod automobila su:

- telematički sustav,
- MP3 *zlonamjerni program* (eng. *malware)*,
- neovlaštene aplikacije,
- daljinsko otključavanje,
- zaključavanje vrata,
- priključak OBD-II.

Upravo su za napade preko priključka OBD-II u sljedećem poglavlju provedena i opisana opsežna ispitivanja. Kratki opis ostalih napadačkih površina dan je u nastavku.



Slika 2. *Napadačke površine modernih automobila*
Izvor: *caranddriver.com*

3.4.1. Telematički sustav

Telematički sustav automobila, koji može obavijestiti policiju da je došlo do sudara, udaljeno onemogućiti ukradeno vozilo i pružiti dijagnostičke informacije vozaču, može također biti povezan s brojnim sustavima u vozilu. Stoga je moguće, nakon što se postigne pristup telematičkom sustavu, upravljati sustavima spojenima na CAN sabirnicu. Napadaču se tada otvaraju velike mogućnosti onesposobljavanja različitih sustava unutar automobila.

Kako bi demonstrirali ovu vrstu napada, istraživači su morali ovladati čitavim telematičkim sustavom i primijeniti obrnuto inženjerstvo na telematički sustav. Iako je provođenje ove vrste napada poprilično složeno, napredni proizvođači su već počeli dodatno pojačavati sigurnost vanjskih komunikacija te mreža koje se nalaze u automobilu.

3.4.2. MP3 zlonamjerni program

Neovlaštenim preuzimanjem glazbe sa servisa za razmjenu datoteka moguće je uz željenu datoteku prenijeti i neželjeni zlonamjerni program koji može tražiti put kako doći do pristupa CAN sabirnici i time ozbiljno ugroziti sigurnost sustava.

Kako informacijsko-zabavni sustavi dobivaju sve više funkcionalnosti, proizvođači automobila ih odvajaju od značajnijih dijelova bez ugrožavanja cjelokupnog sustava. Proizvođači automobila intenzivno rade na poboljšanju sigurnosti svih sigurnosno manjkavih sustava.

3.4.3. Neovlaštene aplikacije

Kao što proizvođači pametnih telefona imaju svoje trgovine za preuzimanje aplikacija u kojima su tisuće programa koje su razvile treće osobe raspoložive za preuzimanje, tako i proizvođači automobila proširuju ponudu informacijsko-zabavnih programa preko programa kojeg je moguće preuzeti. Pa tako neka aplikacija koja sadrži zlonamjerni program može zaraziti automobil bez vlasnikova znanja.

Zaštita od ovakvih vrsta napada dolazi od samih proizvođača automobila koji su vrlo strogi prilikom odabira koje će aplikacije završiti na njihovom sustavu pa tako na primjer Ford i Toyota dozvoljavaju tek malen broj pažljivo probranih programa.

3.4.4. Zaključavanje vrata

U većini modernih automobila mehanizam centralnog zaključavanja je povezan s ostalim sustavima u vozilu. Tako se primjerice vrata mogu automatski zaključati dok je automobil u vožnji ili otključati ako su aktivirani zračni jastuci. Takva međupovezanost teoretski znači da se mehanizam zaključavanja može zloupotrijebiti za pristup ostalim sustavima. Ako ubrzanje može utjecati na centralno zaključavanje automobila, vješti napadač mogao bi upotrijebiti centralno zaključavanje automobila kako bi natjerao automobil na ubrzanje.

Informacijsko-zabavni i dijagnostički sustavi i dalje su povezani fizičkom vezom s modulima koji nadziru važne funkcije, poput upravljanja i kočenja. No kod nekih sustava ova povezanost postoji samo u jednom smjeru te je na taj način povećana sigurnost.

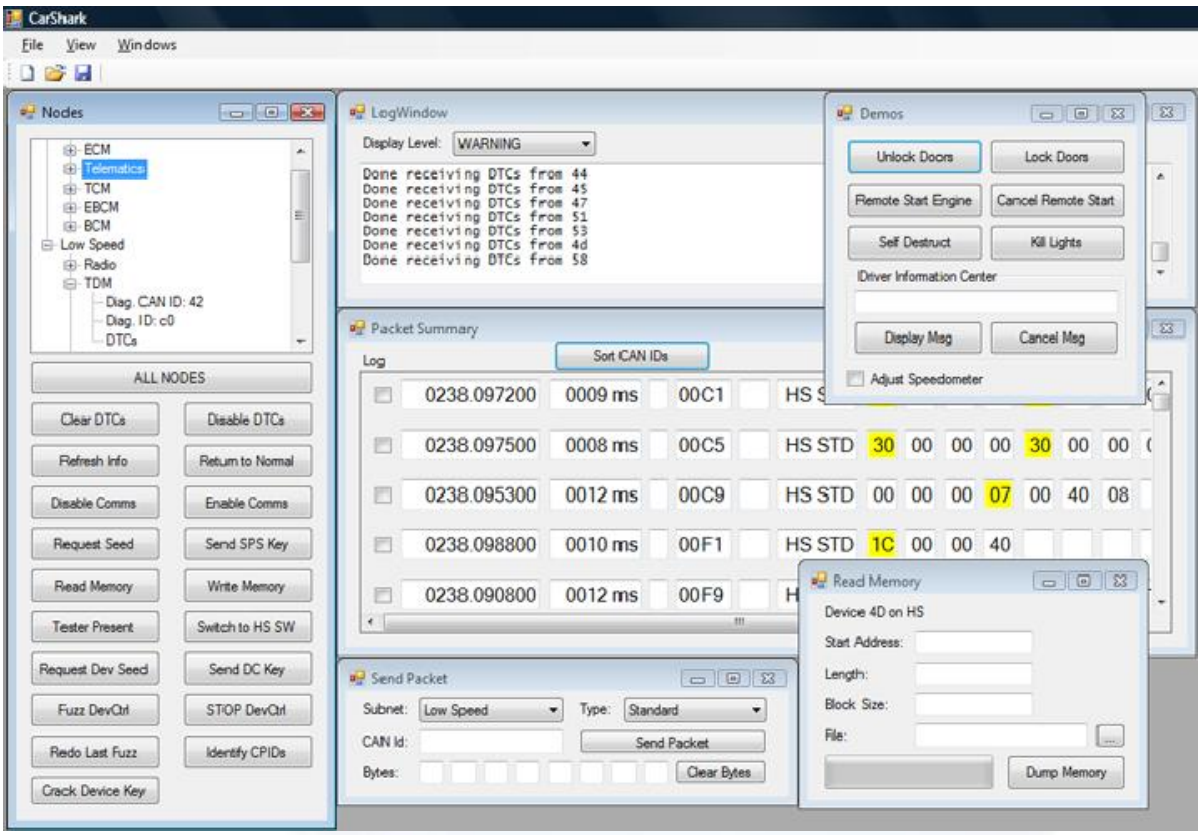
3.4.5. Daljinsko otključavanje

Ova vrsta napada zvuči poput upozorenja koja se pojavljuju u lančanim mailovima, uz jednu važnu činjenicu, točna je. Daljinsko otključavanje namijenjeno je otključavanju i pokretanju automobila samo kad je osoba koja drži daljinski ključ neposredno pokraj vozila ili se nalazi u samom vozilu. Švicarski istraživači pronašli su način kako presresti i produžiti doseg signala na desetak metara koristeći dijelove koji stoje manje od stotinu dolara. Taj pristup ne replicira signal, on samo proširuje doseg signala tako da automobil misli da je daljinski ključ bliže nego što je stvarni slučaj.

Nema mnogo toga što proizvođači mogu učiniti po ovom pitanju. Napadači nisu uspjeli na bilo koji način probiti šifriranje daljinskog ključa, samo su proširili njegov doseg korištenjem radijskog repetitora. Vlasnicima automobila preostaje jedino pojačati pažnju na parkiralištu.

4. Ispitivanje mogućih napada u praksi

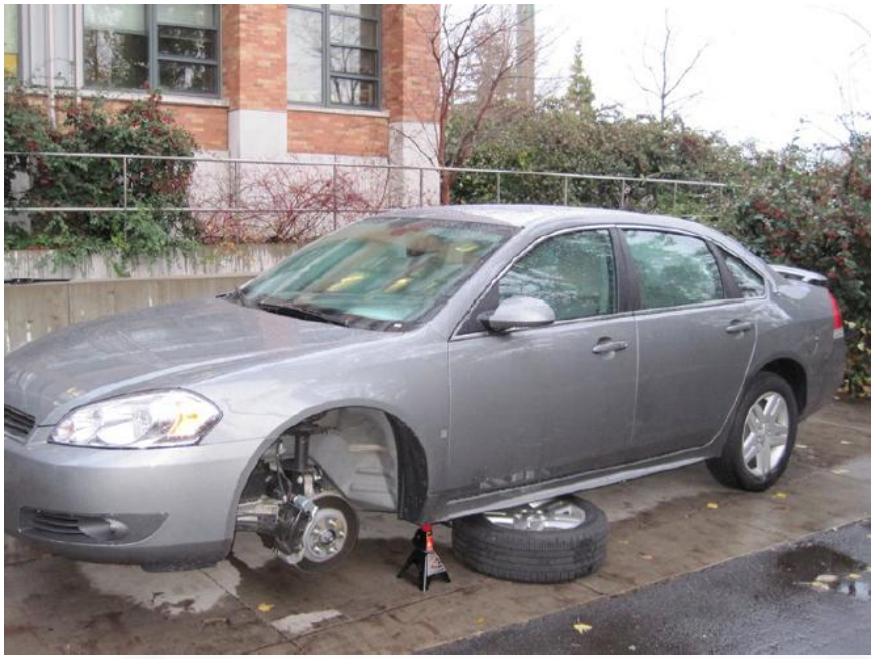
Skupina istraživača sa Sveučilišta u Washingtonu i Sveučilišta u Kaliforniji - San Diego provela je intrigantno ispitivanje, [1]. Na priključak OBD-II priključili su prijenosno računalo te ga bežično povezali s drugim prijenosnim računalom. Koristeći alat za analiziranje i slanje paketa, CarShark, na CAN sabirnici (Slika 3), uspjeli su provesti niz ispitivanja, odnosno, simulirati niz napada na komponente automobila. Ispitivanje u mirovanju proveli su na dva primjerka istog modela, dok su na jednom proveli i ispitivanje u vožnji.



Slika 3. *Screenshot sučelja programa CarShark korištenog u ispitivanju*
Izvor: *Experimental Security Analysis of a Modern Automobile*

4.1. Ispitivanje u mirovanju

Sva početna ispitivanja provedena su nad automobilom u mirovanju koji je radi sigurnosti u mnogim slučajevima bio imobiliziran hidrauličnom dizalicom (Slika 4). Svako ispitivanje na automobilu u mirovanju ponovljeno je i na drugom automobilu, dok su ispitivanja u vožnji provedena samo na prvom automobilu. U nastavku su opisani rezultati ispitivanja nad pojedinim komponentama automobila. Važno je napomenuti da su gotovo svi dobiveni rezultati mogući i pri brzini kretanja vozila od 65 km/h, što je posebno zabrinjavajuće.



Slika 4. *Imobilizirani automobil za potrebe ispitivanja u mirovanju*
Izvor: *Experimental Security Analysis of a Modern Automobile*

4.1.1. Radio

Jedan od prvih napada koji su provedeni bio je napad s ciljem preuzimanja nadzora nad radijom i njegovim ekranom. Omogućeno je potpuno upravljanje radijom, a istovremeno onemogućen bilo kakav korisnikov nadzor nad njim. Primjerice, na ekranu radija ispisivane su proizvoljne poruke, pojačavana je glasnoća bez mogućnosti korisnikovog nadziranja. Budući da radio nadzire i različite zvukove u automobilu, kao što su primjerice zvukovi upozorenja, moguće ih je bilo ponoviti u proizvoljnom trajanju i u proizvoljnim trenucima.

4.1.2. Ploča s instrumentima

Postignut je potpuni nadzor i nad pločom s instrumentima (eng. *Instrument Panel Cluster, IPC*). Omogućeno je ispisivanje proizvoljnih poruka, lažiranje stanja goriva u rezervoaru i lažiranje očitanja brzinomjera, kao i prilagođavanje razine osvjetljenja instrumenata (Slika 5). Kasnije će biti opisan složeniji napad preuzimanja nadzora nad brzinomjerom.

Slika 5. *Prikaz proizvoljne poruke i lažno očitanje brzinomjera*
Izvor: *popularmehanics.com*

4.1.3. Modul upravljanja karoserijom

Preuzimanjem nadzora nad modulom upravljanja karoserijom (eng. *Body Control Module, BCM*) omogućeno je otključavanje i zaključavanja vrata, kao i blokiranje zaključavanja uzastopnim otključavanjem i zaključavanjem vrata, zatim otvaranje prtljažnika, podešavanje razine unutarnjeg i vanjskog osvjetljenja. Omogućeno je i onemogućeno otvaranje prozora te pokretanje brisača, postignuto je trajno izbacivanje tekućine za pranje vjetrobranskog stakla te je preuzet potpuni nadzor nad trubom automobila.

4.1.4. Motor

Niti preuzimanje nadzora nad motorom nije se pokazalo teškim izazovom. Postignuto je trenutno povećanje broja okretaja motora, narušeno je vremensko upravljanje motora, istovremeno su isključeni svi cilindri (čak i kada su se kotači vrtjeli brzinom od 65 km/h na hidrauličkoj dizalici). Postignuto je i gašenje motora tako da se prilikom ponovnog pokretanja čuju neobični zvukovi ili da ga nije uopće moguće ponovno pokrenuti. Dodatno, krivotvoren je paket koji označava aktiviranje zračnih jastuka te je na taj način isključen motor.

4.1.5. Kočnice

Ispitivačima je pošlo za rukom zaključati kočnicu za pojedini kotač, kao i za više njih istovremeno. Također je postignuto oslobađanje kočnica i onemogućavanje njihovog korištenja, čak i kada su se kotači automobila okretali brzinom od 65 km/h. Ono što možda posebno zabrinjava jest činjenica da za preuzimanje nadzora nad motorom i kočnicama automobila nije potrebno više napora nego za ostale komponente.

4.1.6. Sustav grijanja i hlađenja

I nad sustavom grijanja i hlađenja (eng. *Heating, Ventilation, Air Conditioning, HVAC*) lako je preuzet nadzor. Omogućeno je uključivanje i isključivanje grijača i ventilacije te

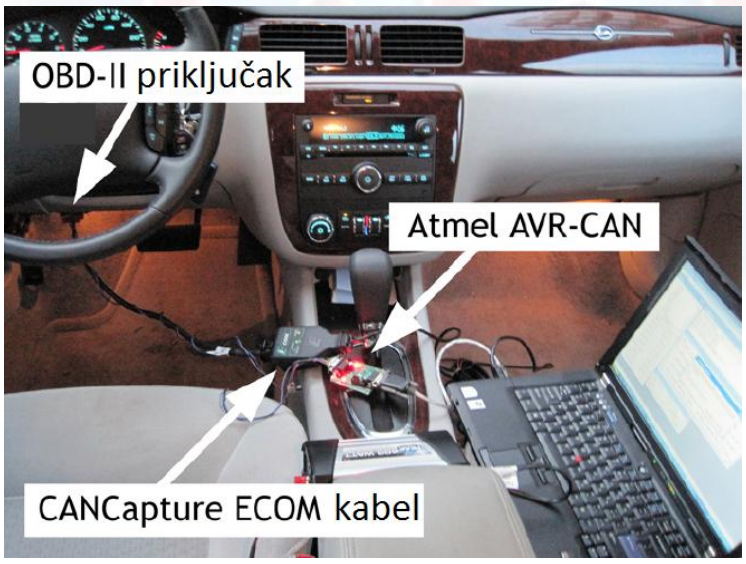
automatskog klima uređaja. U nekim slučajevima nije bilo moguće ručno promijeniti tako postavljene opcije.

4.1.7. Opće uskraćivanje usluge

U jednom nizu ispitivanja onemogućena je komunikacija pojedinih komponenata preko CAN sabirnice. Pritom nisu postojala nikakva ograničenja glede vremena izvođenja napada, to je bilo moguće čak i kada su se kotači automobila okretali brzinom 65 km/h na hidrauličnoj dizalici. Prekid komunikacije iz/prema modulu upravljanja motorom (eng. Engine Control Module, ECM) dok se kotači okreću brzinom od 65 km/h uzrokuje trenutno spuštanje prikaza brzine na 0 km/h. Prekid komunikacije iz/prema modulu upravljanja karoserijom dok se kotači okreću nekom brzinom uzrokuje zamrzavanje podataka na ploči s instrumentima. Automobil je moguće ugasiti u ovom stanju, ali bez ponovnog pokretanja komunikacije iz/prema modulu upravljanja karoserijom nije moguće upaliti automobil. Jednako tako, moguće je spriječiti gašenje automobila, čak i kada se ključem pokuša ugasiti automobil ili se ključ izvadi.

4.2. Ispitivanje u vožnji

Kako bi se osiguralo iscrpno i sigurno ispitivanje prethodno provedenih napada u vožnji bilo je potrebno osigurati otvoren prostor gdje bi se rizici od nesreće sveli na minimum. U tu svrhu ispitivanja su se provodila na sletnoj pisti zatvorenog aerodroma. Kako bi se sigurnost svela na maksimum, osim ispitivanog vozila korišteno je dodatno nadzorno vozilo koje je vozilo usporedno s ispitivanim vozilom. To je omogućilo da samo jedna osoba bude u ispitivanom vozilu. Ispitivanje se provodilo na način da je u ispitivanom automobilu prijenosno računalo preko ODB-II priključka bio spojeno na CAN sabirnicu te je na njemu bio pokrenut program CarShark (Slika 6). Ovim prijenosnim računalom lo daljinski je upravljano pomoću bežične veze s drugim računalom koji se nalazio u nadzornom vozilu. Kako bi se održala bežična veza između prijenosnog računala, nadzorni automobil vozio je usporedno s ispitivanim.



Slika 6. *Spajanje laptopa preko OBD-II priključka na CAN sabirnicu u ispitivanom automobilu*
Izvor*: Experimental Security Analysis of a Modern Automobile*

Gotovo sva ispitivanja koja su provedena nad automobilom u mirovanju uspješno su provedena i nad onim pri vožnji brzinom od 65 km/h (Slika 7). U ovakvom okruženju do izražaja je došla sva opasnost simuliranih napada na automobil. Najopasnijim se pokazalo onesposobljavanje kočnica jer, bez obzira na to kolikom silom vozač pritiskao papučicu kočnice, automobil se nije počeo zaustavljati. Još jedan sličan ispitivani scenarij, ovaj put s različito podešenim kočenjem pojedinih kotača, pokazao se kao vrlo opasan, naročito kod kočenja pri većim brzinama.

Slika 7. *Ispitivanje u vožnji; u pozadini: ispitivani automobil*
Izvor: *Experimental Security Analysis of a Modern Automobile*

Ovo ispitivanje provedeno nad automobilom u vožnji pokazalo je kolika je stvarna opasnost od napada ove vrste na automobile. Mnogi ispitivani slučajevi u praksi su se pokazali mnogo opasnijima nego što se to možda činilo kod ispitivanja automobila u mirovanju. To je napose izraženo kod simuliranja napada onesposobljavanja kočnica. Tek kada se ispitivanje provelo nad automobilom u vožnji bilo je moguće naslutiti razmjere opasnosti koju unosi ova vrsta napada.

4.3. Međudjelovanje više komponenata

U prethodnim poglavljima opisani su mogući slučajevi napada ako je napadač u mogućnosti kontrolirati pojedinu komponentu automobila. U ovom poglavlju razmatraju se slučajevi u kojima napadač u jednom napadu istovremeno napada više komponenati. Upravo ovdje dolazi do izražaja heterogenost pojedinih komponenti automobila koje unatoč tome imaju određena međudjelovanja između sebe. U tom kontekstu važno je sigurnost i otpornost automobila na ovu vrstu napada promatrati s pogleda da je sustav, u ovom slučaju automobil, jedna cjelina sastavljena od mnogo naizgled nezavisnih komponenata. U tablici 1. prikazano je dvanaest važnih elektroničkih upravljačkih jedinica u automobilu s kratkim opisom njihove funkcionalnosti. Uz to navedena je vrsta veze pojedine jedinice sa sabirnicom. CAN sabirnica sastoji se od dva odvojena fizička sloja:

- brza sabirnica - koja se prvenstveno koristi za povezivanje važnih pogonskih sustava,
- spora sabirnica - povezuje manje zahtjevne sustave unutar automobila, osigurava sporiju brzinu prijenosa.

Ako je potrebno, most može preusmjeriti podatke između ovih dviju sabirnica.

Komponenta	Funkcionalnost	Spora sabirnica	Brza sabirnica
ECM	**Modul upravljanja motorom** (eng. *Engine Control Module*); upravlja motorom koristeći informacije sa senzora kako bi odredio količinu goriva, vrijeme paljenja i ostale parametre motora.		X
EBCM	**Modul elektroničkog upravljanja kočnicama** (eng. *Electronic Brake Control Module*); upravlja ABS sustavom sprečavajući zaključavanje kočnica i proklizavanje regulacijom hidrauličkog tlaka.		X
TCM	**Modul upravljanja prijenosom** (eng. *Transmission Control Module*); upravlja elektroničkim prijenosom koristeći podatke sa senzora i ECM-a kako bi odlučio kada i kako promijeniti brzine.		X
BCM	**Modul upravljanja karoserijom**; Upravlja različitim funkcijama vozila, osigurava potrebne informacije te se ponaša kao vatrozid između dvije podmreže.	X	X
Telematika	Omogućuje udaljenu komunikaciju s vozilom preko ćelijske veze.	X	X
RCDLR	**Prijemnik daljinskog upravljanja zaključavanjem** (eng. *Remote Control Door Lock Receiver*); prima signale od daljinskog otključavanja kako bi otključao ili zaključao vrata i prtljažnik. Također bežično prima podatke od senzora za nadzor tlaka u gumama.	X	
HVAC	**Grijanje, ventilacija i klima uređaj**; nadzire temperaturne uvjete u kabini.	X	
SDM	Modul očitavanja i dijagnostike (eng. *Sensing and Diagnostic Module*); upravlja zračnim jastucima i zatezačima sigurnosnih pojaseva.	X	
IPC/DIC	**Instrumentalana ploča/središte informacija za vozača** (eng. *Driver Information Center*); prikazuje vozaču informacije o brzini, razini goriva u rezervoaru i različitim upozorenjima o stanju automobila.	X	
Radio	Osim standardnih radio funkcija stvara i većinu zvukova u kabini.	X	
TDM	**Modul odvraćanja provalnika** (eng. *Theft Deterrent Module*); sprečava uključivanje vozila bez važećeg ključa.	X	

***Tablica 1.** Elektroničke upravljačke jedinice unutar automobila*

4.3.1. Kompozitni napadi

Jedan od primjera kompozitnih napada je upravljanje brzinomjerom tako da pokazuje proizvoljnu brzinu, odnosno da pokazuje neku brzinu udaljenu za proizvoljni odmak od stvarne vrijednosti. Ovakav napad zahtijeva presretanje paketa na sporoj CAN sabirnici koji prenose podatke o trenutnoj brzini i njihovu zamjenu sa zlonamjerno napisanim paketima u kojima se nalaze lažne brzine. Ugrađeni program koji ostvaruje ovu vrstu napada sadrži stotinjak linija koda u programksom jeziku C.

Još jedan primjer kompozitnih napada je napad kojem je cilj gašenje svih unutarnjih i vanjskih svjetala na automobilu nakon što automobil premaši proizvoljnu graničnu brzinu. Ova vrsta napada naročito je opasna noću, u slabo osvijetljenim područjima jer gasi prednja, pomoćna i stop svjetla, unutrašnja svjetla te osvjetljenje ploče s instrumentima.

Lako je moguće zamisliti najcrnji mogući scenarij u kojem se žrtva noću vozi po neosvijetljenom području i odjednom joj se ugase sva svjetla te nije u mogućnosti ništa vidjeti ispred sebe, niti drugi vozači mogu vidjeti takav auto.

Kombinacijom različitih modula upravljanja karoserijom moguće je stvoriti simulaciju 'samouništenja' u kojem je na informacijskom zaslonu prikazano jednominutno odbrojavanje popraćeno zvukovima automobilske trube koje završava gašenjem motora i uključivanjem uzastopnog otključavanja i zaključavanja vrata. Ovaj primjer, koji u općenitom slučaju može biti popraćen proizvoljnim aktivnostima, zahtijevao je manje od dvjesto linija koda dodanog u CarShark. Iz navedenih primjera vidljivo je da je uz minimalne napore moguće napasti automobil i gotovo trenutno ga potpuno onesposobiti.

4.3.2. Premošćivanje unutarnjih CAN mreža

Mnoge dodatne komponente, kao što je primjerice radio, priključuju se na sporu CAN sabirnicu. Kritične komponente, poput upravljanja kočnicama, priključuju se na odvojenu brzu CAN sabirnicu, čijim pristupom upravlja modul upravljanja karoserijom, BCM. Početna pretpostavka da uređaji priključeni na sporu CAN sabirnicu ne mogu štetno djelovati na uređaje priključene na brzu CAN sabirnicu, nakon provedenih ispitivanja, pokazala se pogrešnom. Naime, telematička jedinica automobila je spojena na obje sabirnice te ju je moguće koristiti kao most za prenošenje podataka sa spore na brzu CAN sabirnicu. Na ovaj način u potpunosti je premošćen BCM ulaz. Ovakav slučaj treba razmatrati s posebnom pažnjom, naročito zbog porasta mogućih dodataka koji se priključuju na sporu sabirnicu.

4.3.3. Čuvanje i brisanje koda

Još jedna metoda napada je metoda umetanja i čuvanja zlonamjernog koda u neku od komponenata automobila, primjerice u telematičku jedinicu. Zlonamjerni kod može postojati istovremeno s kodom telematičke jedinice. Postojeći napad moguće je proširiti u svrhu otežavanja forenzičke istrage. Tako primjerice zlonamjerni kod može izvesti neku akciju za koju je programiran i nakon toga izbrisati svaki trag svoga postojanja na tom uređaju. Navedeni scenarij predstavlja forenzičarima gotovo nemoguću zadaću otkrivanja uzroka eventualne nesreće.

5. Budućnost automobilske sigurnosti

Potpuno je izvjesno da će automobili u budućnosti imati još više temeljnih funkcija ostvarenih pomoću računala i uz naprednije mogućnosti. Primjerice, neki automobili već danas koriste računalo kako bi se parkirali, prilagodili razinu osvjetljenja prednjih svjetala prilikom približavanja vozila iz suprotnog smjera ili pak automatski uključuju kočnice kako bi izbjegli mogući sudar. Stoga je razumno pretpostaviti da će se nastaviti upotreba i razvoj računala za ovakve i slične svrhe.

Moderni automobili postaju sve povezaniji s vanjskim svijetom i realno je za očekivati da će se taj trend nastaviti i u budućnosti. Brojni današnji navigacijski sustavi informiraju vozača o stanju u prometu, bežični senzori pritiska prenose digitalne signale s informacijama o tlaku u gumama, također, mnogi automobili nude Bluetooth sučelje za podršku poziva slobodnih ruku (eng. hands free). Telematički sustavi pružaju još naprednije komunikacijske mogućnosti. Konačno, zamjetna pažnja posvećuje se razvoju novih komunikacijskih sposobnosti između vozila kojima bi se spriječile gužve i izbjegle nesreće. Vrlo je izvjesno da će se u budućnosti nastaviti ovaj trend sve veće povezanosti.

Istraživanja u budućnosti će se nastaviti usmjeravati na teme opisane u ovom dokumentu i na razvoj novih sigurnosnih tehnologija za buduće automobile. Pritom je važno naglasiti da najvjerojatnije neće postojati jedinstveno rješenje za sve navedene sigurnosne probleme niti da će do tog rješenja doći jedna skupina istraživača. Automobilsko okruženje predstavlja novi izazov za računalnu sigurnost te će sigurno u budućnosti doći do snažnog razvoja ove grane računalne sigurnosti. Rješavanju ovog problema trebale bi pristupiti sve interesne skupine kojih se to tiče, ne ograničavajući se samo na istraživače i automobilsku industriju u cjelini, već bi se u istraživanja trebale uključiti vlade, osiguravajuća društva, skupine koje se brinu za javne interese te cjelokupna javnost.

6. Zaključak

Nakon svih navedenih metoda i slučajeva napada na automobile, postavlja se pitanje kolika je stvarna opasnost da se dogodi neki od mogućih napada. Stručnjaci u ovom području se ipak slažu oko zaključka da trenutno ne postoji velika opasnost, no uvijek treba biti na oprezu. Kao glavne premise ovog zaključka navode činjenice da je za hakiranje automobila potrebno puno vremena, truda i novaca. No unatoč svemu, proizvođači automobila posvećuju i nastavit će posvećivati sve više pažnje povećavanju sigurnosti računalnih sustava u automobilima.

Ispitivanje koje su proveli istraživači s dva ugledna američka sveučilišta na prvi pogled daje zastrašujuće rezultate. Kroz svoje ispitivanje pokazali su da ne postoji računalni sustav unutar automobila kojemu nije moguće pristupiti i izvršiti neku vrstu napada uz uvjet da imamo pristup priključku automobila OBD-II. Upravo taj uvjet čini ove napade malo vjerojatnima u stvarnosti jer je teško vjerovati da bi prijenosno računalo priključeno na priključak automobila OBD-II mogao proći nezapaženo. Jednako tako, postavlja se pitanje kako bi napadač uspio doći do pristupa tom priključku.

Razvoj računalne tehnologije u automobilskoj industriji dosegao je visoku razinu pri kojoj se na automobile u području njihove sigurnosti i zaštite sve češće gleda gotovo jednako kao na osobna i prijenosna računala i poslužitelje. Jasno je izražena potreba za poboljšanjem i razvojem sigurnosti automobilskih sustava. Jedna vrlo važna činjenica je u svemu ovome možda i nehotice stavljena po strani, za razliku od računala i računalnih sustava, hakerski napadi na automobile mogu kao posljedice imati ljudske žrtve. A sigurnost ljudskih života trebala bi biti glavni motiv razvoja ovog područja koje u sebi krije mnoge pozitivne, ali nažalost, u pogrešnim rukama, i negativne mogućnosti.

Leksikon pojmova

DOS napad (Napad uskraćivanjem usluge)

Nekada poznata pod imenom NBS (National Bureau of Standards), NIST je agencija koja se bavi mjeriteljstvom, standardima i tehnologijama u cilju poboljšanja ekonomske sigurnosti i kvalitete života.

http://en.wikipedia.org/wiki/Denial-of-service_attack

RFID (Radio-frequency identification)

Čip tehnologija koja omogućava prijenos podataka sa čipa do čitača putem radijskih frekvencija. Trenutno se najviše koristi za obilježavanje proizvoda u skladištima i prodavaonicama, a u zadnje vrijeme postaje popularan za identifikaciju osoba.

http://www.aimglobal.org/technologies/RFID/what_is_rfid.asp

Virus (Računalni virus)

Virusi su programi koji se mogu kopirati i zaraziti računalo bez znanja ili dopuštenja korisnika. Računalo se može zaraziti na razne načine preko Internet-a, CD-a, USB-a... Virusi dolaze većinom sa drugim programima, kao što su npr. Trojanski konji kako bi maskirali svoj rad i kako bi ih bilo još teže za otkriti. Namjene virusa su različite, mogu služiti samo kako bi radili štetu no neki su manje štetni i samo usporavaju računalo i smetaju korisniku u radu. Virusi se spremaju u memoriju računala i pokreću se s operacijskim sustavom i inficiraju programe koji se pokreću.

http://www.ust.hk/itsc/antivirus/general/whatis.html

Reference

[1] Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H. i Savage, S. Experimental Security Analysis of a Modern Automobile, 2010.
http://www.autosec.org/pubs/cars-oakland2010.pdf, siječanj 2012.

[2] Koscher, K.,Czeskis, A., Roesner, F., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H. i Savage, S. Comprehensive Experimental Analyses of Automotive Attack Surfaces, 2011.
http://www.autosec.org/pubs/cars-usenixsec2011.pdf, siječanj 2012.

[3] Center for Automotive Embedded Systems Security, FAQ
http://www.autosec.org/faq.html, siječanj 2012.

[4] Keith Barry: Can Your Car Be Hacked?, srpanj 2011.
http://www.caranddriver.com/features/can-your-car-be-hacked-feature, siječanj 2012.

[5] Glenn Derene: How Vulnerable Is Your Car to Cyber Attack?, lipanj 2010.
http://www.popularmechanics.com/technology/how-to/computer-security/how-vulnerable-is-your-car-to-cyber-attack, siječanj 2012.

[6] Willie D. Jones: Cars: The Next Victims of Cyberattacks, siječanj 2012.
http://spectrum.ieee.org/tech-talk/computing/embedded-systems/cars-the-next-victims-of-cyberattacks, siječanj 2012.

[7] Honda Fan Club, Rječnik pojmova
http://www.hondafanclub.hr/index.php/rjenik-pojmova, siječanj 2012.