# Naslov seminarskog rada

Seminarski rad u okviru kursa
Metodologija stručnog i naučnog rada
Matematički fakultet

Prvi autor, drugi autor (treći autor)
kontakt email prvog, drugog (trećeg) autora

9. april 2015.

## Sadržaj

# 1 Uvod

# 2 Izazovi

[1]

Svaki računarski sistem može biti preplavljen propustima i slabostima koje napadač može da iskoristi ako je povezan na sistem. Elektronskim kontrolnim jedinicama (EKJ ili ECU na engleskom) nije lako pristupiti van vozila, te implementacija bezbednosnih mehanizama u računarskim mrežama u automobilima nije bila velika briga proizvođača.

Umrežavanje je trend današnjice. Moderna vozila često poseduju interfejse koji omogućavaju ili žičanu ili bežičnu komunikaciju. Ovime su mreže u automobilima prestale da budu zatvorene i sajber-napadi su postali realnost.

## 2.1 Razlozi za napade

Razmotrimo prvo koje sve motive napadači računarskih mreža u automobilima mogu imati.

*Krađa*

Napadač može da iskoristi neki prisutni propust u bežičnoj komunikaciji i na taj način tiho i neprimetno otključa automobil i zatim deaktivira alaram.

*Elektronska podešavanja*

Napadač je upravo vlasnik ciljanog automobila. Vlasnik može da pristupi kodu ili podacima i promeni ih. Na primer, može da smanji kilometražu automobila pre prodaje, izvrši podešavanje motora i dobije više snage ili instalira nedozvoljene programe u komandnoj tabli. Takođe, mogu se instalirati jeftine AFTERMARKET komponente umesto skupljih koje je odobrio proizvođač.

*Sabotaža*

Sabotaža podrazumeva deaktivaciju EKJ, menjanje njihovog softvera ili dos (denial of service) napade na mrežu. Posledice ovih napada se protežu od minornih (zaključavanje klima uređaja) do potencijalno smrtonosnih (zaključavanje kočnica). Ali čak i napadi koji uzrokuju samo male neprijatnosti mogu znatno da utiču na reputaciju proizvođača.

*Intelektualna krađa*

Napadač može da pokuša da pristupi poverljivim informacijama o EMBEDDED mreži ciljanog vozila. To se može postići prisluškivanjem magistrale ili pristupanjem izvornom kodu neke EKJ. Ovakvi napadi mogu da omoguće proizvodnju falsifikovanih EKJ, kao i širenje informacija o propustima u bezbednosti drugim napadačima.

*Povreda privatnosti*

Sa povećanjem broja elektronskih komponenti, povećava se i količina privatnih informacija koje te komponente skupljaju. Napadač može da pristupi telefonskom imeniku vlasnika kao i istoriji poziva, istoriji GPS koordinata ili omiljenim radio frekvencijama.

*Intelektualni izazovi*

Mnogi napadači su prosto motivisani izazovom preuzimanja kontrole nad vozilom. Postoje mnogi primeri ovakvih napada kroz istoriju računarstva.

Naravno, jedan napadač može imati i više motiva.

## 2.2 Unutrašnji napadi

Kao što je ranije pomenuto, neki bezbednosni mehanizmi su implementirani u posotjeće računarske mreže u vozilima. Bezbednost je postala značajan problem s obzirom da posledice napada mogu biti veoma ozbiljne, a napadi se mogu lakše izvesti zahvaljujući rapidnoj evoluciji mreža.

*Ranjivost magistrale*

Već su prikazane ranjivosti koje postoje u trenutnim protokolima, sa fokusom na CAN. Iako neke EKJ imaju specifične bezbednosne mehanizme (kao što je autentikacija uređaja), pokazano je da CAN ne može da garantuje sledeće osobine:

- Poverljivost:
  Dizajn je takav da se svaka poruka poslata na CAN i fizički i logički šalje (BROADCAST) svakom čvoru. Ovo omogućava zlonamernim čvorovima da prisluškuju magistralu i čitaju sadržaj svakakog okvira (FRAME).
- Autentikacija:
  CAN okvir ne podrazumeva polje za autentikaciju svog pošiljaoca. Dakle, svaki čvor može da pošalje poruku koju bi trebalo da može da šalje samo jedan specifičan čvor.
- Dostupnost:
  Veoma je lako izazvati dos napad na magistrali. Na primer, neka jedinica može da preplavi magistralu okvirima visokog prioriteta i time zaustavi transmisije ostalih EKJ.
- Integritet:
  CAN koristi CRC (cyclic redundancy check) da proveri da li je poruka promenjena usled greške, ali ovaj mehanizam ne može da spreči napadača koji želi da promeni ispravnu poruku jer je lako napraviti ispravan CRC za lažnu poruku.

# Literatura

[1] I. Studnia, V. Nicomette, E. Alata, Y. Deswarte, M. Kaâniche, and Y. Laarouchi. Survey on security threats and protection mechanisms in embedded automotive networks. In *2013 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W)*, pages 1–12, June 2013.