|  |  |  |
| --- | --- | --- |
|  | УНИВЕРЗИТЕТ У НОВОМ САДУ  **ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА У НОВОМ САДУ** |  |

Филип Дутина

**Једно решење програмске подршке за безбедан пренос података путем BroadR-Reach интерфејса**

ДИПЛОМСКИ РАД

- Основне академске студије -

Нови Сад, 2018

|  |  |  |  |
| --- | --- | --- | --- |
| Редни број, **РБР**: | |  | |
| Идентификациони број, **ИБР**: | |  | |
| Тип документације, **ТД**: | | Монографска документација | |
| Тип записа, **ТЗ**: | | Текстуални штампани материјал | |
| Врста рада, **ВР**: | | Завршни (Bachelor) рад | |
| Аутор, **АУ**: | | Филип Дутина | |
| Ментор, **МН**: | | Доц. др Богдан Павковић | |
| Наслов рада, **НР**: | | Једно решење програмске подршке за безбедан пренос података путем BroadR-Reach интерфејса | |
| Језик публикације, **ЈП**: | | Српски / латиница | |
| Језик извода, **ЈИ**: | | Српски | |
| Земља публиковања, **ЗП**: | | Република Србија | |
| Уже географско подручје, **УГП**: | | Војводина | |
| Година, **ГО**: | | 2018 | |
| Издавач, **ИЗ**: | | Ауторски репринт | |
| Место и адреса, **МА**: | | Нови Сад; трг Доситеја Обрадовића 6 | |
| Физички опис рада, **ФО**: (поглавља/страна/ цитата/табела/слика/графика/прилога) | | **<уписати статистику>** | |
| Научна област, **НО**: | | Електротехника и рачунарство | |
| Научна дисциплина, **НД**: | | Рачунарска техника | |
| Предметна одредница/Кqучне речи, **ПО**: | | Безбедан ренос података, енкрипција/декрипција, zFAS развојна плоча | |
| **УДК** | |  | |
| Чува се, **ЧУ**: | | У библиотеци Факултета техничких наука, Нови Сад | |
| Важна напомена, **ВН**: | |  | |
| Извод, **ИЗ**: | | Задатак рада је дизајнирање и имплементација безбедног преноса података са наменске платформе на рачунар. Енкрипција података који се преносе је неопходна како би се осигурала безбедна и сигурна комуникација. Пренос података се врши путем BroadR-Reach интерфјеса и IPv6 протокола. | |
| Датум прихватања теме, **ДП**: | |  | |
| Датум одбране, **ДО**: | |  | |
| Чланови комисије, **КО**: | Председник: | **<име председника комисије>** |
|  | Члан: | **<име члана комисије>** | Потпис ментора |
|  | Члан, ментор: | **<име ментора>** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Accession number, **ANO**: | |  | |
| Identification number, **INO**: | |  | |
| Document type, **DT**: | | Monographic publication | |
| Type of record, **TR**: | | Textual printed material | |
| Contents code, **CC**: | | Bachelor Thesis | |
| Author, **AU**: | | Filip Dutina | |
| Mentor, **MN**: | | Bogdan Pavković, Phd | |
| Title, **TI**: | | One software solution for safe data transmision via BroadR-Reach interface | |
| Language of text, **LT**: | | Serbian | |
| Language of abstract, **LA**: | | Serbian | |
| Country of publication, **CP**: | | Republic of Serbia | |
| Locality of publication, **LP**: | | Vojvodina | |
| Publication year, **PY**: | | 2018 | |
| Publisher, **PB**: | | Author’s reprint | |
| Publication place, **PP**: | | Novi Sad, Dositeja Obradovica sq. 6 | |
| Physical description, **PD**: (chapters/pages/ref./tables/pictures/graphs/appendixes) | | **<upisati statistiku>** | |
| Scientific field, **SF**: | | Electrical Engineering | |
| Scientific discipline, **SD**: | | Computer Engineering, Engineering of Computer Based Systems | |
| Subject/Key words, **S**/**KW**: | | Safe data transmission, encryption/decription, zFAS embedded board | |
| **UC** | |  | |
| Holding data, **HD**: | | The Library of Faculty of Technical Sciences, Novi Sad, Serbia | |
| Note, **N**: | |  | |
| Abstract, **AB**: | | This paper presents design and implementation of safe data transmission from embedded board to the PC. Data encryption is necessary in order to secure safe communication. Data transmission is done via BroadR-Reach interface and IPv6 protocol. | |
| Accepted by the Scientific Board on, **ASB**: | |  | |
| Defended on, **DE**: | |  | |
| Defended Board, **DB**: | President: | **<ime predsednika komisije>** |
|  | Member: | **<ime člana komisije>** | Menthor's sign |
|  | Member, Mentor: | **<ime mentora>** |  |

**Zahvalnost**

Srdačno se zahvaljujem mentoru Doc. dr Bogdanu Pavkoviću na stručnoj pomoći tokom izrade ovog rada.

Posebno se zahvaljujem Draganu Radanoviću na stručnoj pomoći, stalnoj podršci, strpljenju, utrošenom vremenu, razumevanju i savetovanju tokom izrade ovog diplomskog rada.

Takođe se zahvaljujem Institutu RT-RK na ukazanoj prilici da se bolje upoznam sa načinom rada u inženjerskom okruženju i na omogućenom usavršavanja znanja iz date oblasti.

Na kraju, najveće hvala Tatjani, Milošu, Vjeri, Mirku, Jeleni i svima onima koji su mi bili podrška, potpora i motivacija tokom školovanja.

**Sadržaj**

[1. Uvod 1](#_Toc472220115)

[2. Poglavlje 1](#_Toc472220116)

[3. Zaključak 1](#_Toc472220117)

[4. Literatura 1](#_Toc472220118)

**Spisak slika**

**Error! No table of figures entries found.**

**Spisak tabela**

**Error! No table of figures entries found.**

**Skraćenice**

**zFAS** - *Zentrale Fahrerassistenz Steuerung*, centralni procesor u automobilu

**TCP** - *Transmission Control Protocol*, mrežni protokol

**IPv6 -** *Internet Protocol Version 6,* šesta revizija Internet Protokola

**RSA -** *Rivest – Shamir – Adleman algorithm*, algoritam asimetrične enkripcije

# Uvod

Da bi autonomni automobili preuzeli primat na putevima i postali deo svakodnevice, jedan od najvećih izazova sa inženjerske tačke gledišta svakako jeste prenos, skladištenje i manipulacija podacima. Navodno, devedeset minuta vožnje jednog autonomnog automobila predstavlja ekvivalet korišćenju milion pametnih telefona u rasponu od dvadeset i četiri časa po obimu obrađenih podataka. U savremenim automobilima može se nalaziti više desetina, sve češće i više stotina elektronskih sistema, koji međusobno komuniciraju preko automobilskih mreža (CAN, CAN HS, Ethernet, LIN itd.). Sa stanovništa bezbednosti od neželjenog pristupa, sigurnost automobilskih mreža nije na nivou kao u potrošačkoj industriji već mora biti na mnogo višem nivou. Ovde je potrebno obezbediti dodatnu zaštitu, kao i šifrovanje podataka, kako bi se onemogućila, ili makar znatno otežala manipulacija podacima koji se čuvaju u automobilu, kao što su dijagnostički podaci, rezultati očitavanja senzora, podaci o izvršenim popravkama i servisima, ukupna pređena kilometraža vozila, i slično.

U ovom radu biće opisano jedno rešenje programske podrške za bezbedan prenos podataka sa namenske ploče na računar, njihova enkripcija pre slanja i dekripcija po primanju, putem BroadR-Reach interfejsa i IPv6 protokola. Rešenje je realizovano na *zFAS* razvojnoj ploči.

Rad je sačinjen od ----XY---- poglavlja. Prvo poglavlje sadrži kraći uvod u rad, motivaciju i opis samog rada.

U drugom poglavlju se nalaze teorijske osnove koje su neophodne za shvatanje rada – opis *zFAS* razvojne ploče, pojašnjenje *TCP* i *IPv6* protokola kao i nekoliko reči o asimetričnoj *RSA* enkripciji.

Treće poglavlje sadrži koncept rešenja.

Četvrto poglavlje daje detaljan opis programskog rešenja sa dubljim analizama napisanih funkcija i kritičnih sekcija koda.

U petom poglavlju su predstavljeni rezultati testnih slučajeva i njihovo tumačenje.

Šesto poglavlje sadrži kratak pregled onoga što je urađeno u ovom radu i ideje na koji način bi programska podrška mogla dalje da se razvija.

U sedmom poglavlju je dat spisak korišćene literature tokom izrade ovog rada.

# Teorijske osnove

## zFAS razvojna ploča

## TCP protokol

TCP predstavlja protokol transportnog nivoa. Ovaj protokol omogućava istovremeno dvosmernu pouzdanu komunikaciju između klijenta i servera. Komunikacija je realizovana u vidu konekcije koja se uspostavlja pomoću metode rukovanja (eng. Handshaking). Iz tog razloga ne podržava multicast.

NASTAVITI PISANJE O TCP-u SA SAJTA KATEDRE!

# Zaključak

# Literatura

1. Vladimir Kovačević: *Logičko projektovanje računarskih sistema I –projektovanje digitalnih sistema*, Univerzitet u Novom Sadu, Fakultet Tehničkih Nauka, 2001