|  |  |  |
| --- | --- | --- |
|  | 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

**MIT -** *The Massachusetts Institute of Technology*, Tehnološki institut Masačusetsa

# 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

---OVDE TREBA NAPISATI PONESTO O ZFAS PLOCI!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!---

mogu pisati jos i o 26262, autosaru, misri, broadr-reachu....................................

## BroadR-Reach interfejs

## 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.



Slika 2.1 Segmentacija

*TCP* koristi **segment** za jedinicu prenosa (jedinice podataka transportnog sloja). Proces podele originalne poruke aplikativnog nivoa na segmente naziva se **segmentacija**. *TCP* omogućava praćenje poslatih paketa, kontrolu toka komunikacije, kao i redosleda pristiglih segmenata.

*TCP* definiše uslugu pouzdane isporuke toka (engl. *stream*) korisničkih podataka. Osobine *TCP*-a su:

• Obavlja kontrolu toka podataka, *TCP* obezbeđuje komunikaciju sistema različitih brzina.

• Osnovna jedinica prenosa *TCP*-a je segment podataka. Segmenti se koriste za prenos upravljačke informacije (npr poruke za uspostavu i raskid veze), ili za prenos podataka.

• Format segmenta je izabran tako da je moguće potvrđivanje podataka iz jednog smera, njihovim uključivanjem u zaglavlje segmenata koji se šalju u drugom smeru.

• Kontrola toka je realizovana tako što prijemnik oglašava količinu podataka koju je spreman da primi.

• *TCP* takođe podržava poruke van opsega (engl. “*out of band*”), koje služe za slanje urgentnih podataka i za forsiranje isporuke korišćenjem (engl. “*push*”) podataka.



Slika 2.2 Izgled *TCP* segmenta

Na slici 2.2 je dat prikaz *TCP* segmenta, koji se sastoji iz zaglavlja i dela u kome se nalaze podaci. Zaglavlje se sastoji iz:

• Source port - izvorišni port (port pošiljaoca). Port ima ulogu u identifikaciji aplikacije.

• Destination port - odredišni port (port primaoca).

• Sequence number - broj prvog bajta segmenta u okviru toka podataka. Broj sekvence omogućava praćenje toka podataka. Inicijalni broj sekvence se bira nasumično, kako bi se otklonila mogućnost interferencije između različitih konekcija.

o syn = 1 - Inicijalni broj sekvence.

o syn = 0 - Akumulirani broj sekvence.

• Acknowledgement number - broj sekvence narednog segmenta koji se očekuje. Segmenti koji pristignu van redosleda, u zavisnosti od implementacije, mogu se odbaciti ili čuvati.

• Header Length - dužina zaglavlja. 3

• Reserved - rezervisano za buduću upotrebu.

• Control bits - ukazuje na funkciju i namenu segmenta.

o ack - ukazuje na validnost vrednosti potvrde (acknowledgment-a).

o syn, rst i fin - omogućavaju uspostavljanje i prekid konekcije.

o psh - ukazuje prijemnoj strani da se momentalno pošalju podaci višem sloju.

o urg - ukazuje na postojanje urgentnih podataka u segmentu.

• Window - maksimalan broj bajtova koje je moguće poslati, a da prethodno nije potvrđen njihov prijem.

• Checksum - koristi se za za proveru da li se desila greška poruke nad zaglavljem i podacima prilikom prenosa.

• Urgent - lokacija poslednjeg bajta koji je markiran kao urgentan.

• Options - dodatne opcije.

• Application data - podaci viših slojeva.

### Uspostavljanje veze

Komunikacija klijenta i servera preko *TCP* protokola zahteva uspostavu veze koja se ostvaruje tako što se između predajne i prijemne strane iz tri puta razmene poruke sa podešenih odgovarajućim kontrolnim bitima (*TCP* *three-way handshake*):

• Predajna strana A šalje poruku sa podešenim kontrolnim bitom SYN = 1, ostali su podešeni na 0, pri čemu nasumično odabere redni broj segmenta (SEQa).

• Prijemna strana B odgovara porukom sa kontrolnim bitima SYN i ACK = 1, takođe nasumično bira broj segmenta (SEQb), a za ACK uzima broj ACK = (SEQa) + 1. Na ovaj način je uspostavljena veza na liniji od predajne ka prijemnoj strain.

• Slanjem poruke sa podešenim kontrolnim bitom SYN = 1 od prijemne strane, ona zahteva da predajna strana potvrdi uspostavljanje veze od prijemne ka predajnoj strani. Predajna strana to čini slanjem poruke sa podešenim kontrolnim bitom ACK = 1 i 4 uzima vrednost ACK broja ACK = (SEQb) + 1. Na ovaj način je uspostavljena konekcija između klijenta i servera.



Slika 2.3 *TCP* uspostava veze

### Prekid veze

Prekid veze se ostvaruje u četiri koraka sledećim redosledom:

1. Klijent inicira prekid klijent-server konekcije,

2. Server potvrđuje zahtev za prekid klijent-server konekcije,

3. Server šalje zahtev za prekid server-klijent konekcije,

4. Klijent odgovara na zahtev za prekid server-klijent konekcije. [1]



Slika 2.4 *TCP* prekid veze

## IPv6 protokol

Internet protokol verzija 6 (*IPv6*) je protokol sloja mreže, naslednik internet protokola vrezije 4 (*IPv4*), osmišljen od strane IETF-a (engl. *Internet Engineering Task Force*).

### IPv6 adresa

*IPv6* je novi (ali ne još široko korišćen) standardni internet protokol, gde su adrese 128 bita široke, što bi, čak i sa velikim dodelama netblokova, trebalo da zadovolji blisku budućnost. Teoretski, postojalo bi tačno 2128, ili 3.403×1038 unikatnih adresa domaćinskih interfejsa. Kada bi zemlja bila sačinjena kompletno od zrna peska od 1cm³, onda bi mogla da se dodeli jedinstvena adresa svakom zrnu u 300 miliona planeta veličine zemlje. Ovaj veliki prostor za adrese teško da će ikada biti potpuno popunjen. Adresa verzije 6 se piše kao osam četvorocifrenih heksadecimalnih brojeva (8 puta po 16 bitova) odvojenih dvotačkama. Jedan niz nula po adresi može da se izostavi, pa je 1080::800:0:417A isto što i 1080:0:0:0:0:800:0:417A. Globalne adrese koje se šalju ka jednom odredištu se sastoje iz dva dela: 64-bitni deo za rutiranje i 64-bitni identifikator domaćina.

### Struktura IPv6 paketa

Jedan *IPv6* paket ima sledeću opštu formu:



Slika 2.5 Izgled *IPv6* paketa

Jedino potrebno zaglavlje se odnosi na *IPv6* zaglavlje. Ovo je fiksna veličina sa dužinom od 40 bajtova, u poređenju sa 20 bajtova pomoćnog dela *IPv4*. Sledeća produžena zaglavlja su definisana kao:

• Zaglavlje *Hop-by-Hop* opcija: Definišu specijalne opcije koje zahtevaju hop-by-hop procesiranje.

• Zaglavlje rutiranja: Obezbeđuje prošireno rutiranje, slično izvorišnom rutiranju u *IPv4*.

• Zaglavlje fragmenata: Sadrži informacije o fragmentaciji i ponovnom sklapanju.

• Zaglavlje autentičnosti: Ovezbeđuje integritet i autentičnost svakog paketa.

• Zaglavlje enkapsulacije sigurnosti podatka: Obezbeđuje privatnost.

• Zaglavlje odredišnih opcija: Sadrži fakultativne informacije koje će ispitati odredišni čvor.



Slika 2.6 Primer *IPv6* paketa sa uključenim zaglavljima

*IPv6* zaglavlje i svako produženo zaglavlje sadrže polje *sledeće zaglavlje*. Ovo polje identifikuje tip sledećeg zaglavlja. Ako je sledeće zaglavlje jedno od produženih zaglavlja, onda ovo polje sadrži identifikator tipa tog zaglavlja. U protivnom, ovo polje sadrži identifikator protokola za protokol višeg sloja koji koristi *IPv6* (obično protokol transportnog sloja), koriste se iste veličine kao i polja *IPv4* protokola. Na slici, protokol višeg sloja je *TCP*, tako da se podaci viših slojeva koje nosi *IPv6* paket sadrže od zaglavlja *TCP*-a koje prati blok aplikacionih podataka. [2]

## Asimetrična RSA enkripcija, osobine i primena

Enkripcija (engl. *encryption*) ili šifrovanje je proces u kriptografiji kojim se vrši izmena podataka tako da se podaci, ili poruke, učine nečitljivim za osobe koje ne poseduju određeno znanje (ključ). Na taj način se dobija šifrovana informacija. Da bi ovi podaci postali razumljivi i upotrebljivi, potrebno je da se dekodiraju. Dekodiranje se vrši procesom suprotnim od enkripcije koji se naziva dekripcija (engl. *decryption*).

### Elementi enkripcije

Svi sistemi enkripcije imaju u svojoj osnovi sledeće zajedničke elemente:

• Algoritam: Funkcija, obično sa jakom matematičkom osnovom, koja obavlja zadatak enkripcije podataka;

• Ključevi: Koriste se zajedno sa algoritmima enkripcije i određuju način na koji su podaci šifrovani;

• Dužinaključa: Enkripcioni ključevi imaju određenu dužinu u zavisnosti od toga koji enkripcioni sistemi se koriste. Dužina se meri brojem bitova ,a što su duži ključevi, teži su za oštećenje sistema enkripcije;

• Otvoren tekst (engl. *Plaintext*): Informacije koje želimo da šifrujemo;

• Šifrovan tekst (engl. *Ciphertext*): Informacije nakon šifrovanja. [3]

### Osobine RSA enkripcije

Postoje dve osnovne vrste enkripcije, simetrična i asimetrična enkripcija. Kod simetrične enkripcije se i za šifrovanje i za dešifrovanje koristi ista šifra (ključ), i samim tim što obe strane koriste isti ključ i za enkripciju i za dekripciju proboj sistema je znatno olakšan. Kod asimetrične enkripcije postoji poseban ključ samo za šifrovanje i drugi koji služi samo za dešifrovanje. Ova dva ključa nazivaju se još *javni* i *tajni* ključ. Tajni ključ se dodeljuje onda kada se vrši enkripcija i na osnovu njega se generiše javni ključ, koji koristi strana koja treba da pročita podatke. *RSA* (akronim od Rivest – Shamir – Adleman) predstavlja jedan od najčešće korištenih algoritama za asimetričnu enkripciju, razvijen od strane trojice stručnjaka sa *MIT*-a 1977. godine i u sledećem poglavlju će detaljno biti opisan način na koji funkcioniše.



Slika 2.7 Prikaz *RSA* enkripcije i dekripcije

### Algoritam RSA enkripcije

Kao što je već rečeno, kod *RSA* enkripcije se koriste dva ključa, javni i tajni. Javni ključ je dostupan svima i on se koristi za enkriptovanje poruka. Poruke koje su enkriptovane javnim ključem mogu se dekriptovati jedino tajnim ključem. Ovaj par ključeva se generiše na sledeći način:

1. Biraju se dva nasumična velika prosta broja i .
2. Računa se .
3. Računa se vrednost Ojlerove fi funkcije .
4. Bira se ceo broj takav da zadovoljava uslov i i ne smeju imati zajednički faktor osim broja **.** Par i predstavljaju javni ključ.
5. Na kraju se računa tako da zadovoljava uslov za neki ceo broj . Par i se čuvaju kao tajni ključ.

Formula koja se koristi za enkripciju poruke je , a da bi se iz enkriptovane poruke došlo do originalne poruke , neophodno je uraditi sledeće . [4]

Kod *RSA* enkripcije se postavlja pitanje zašto se koriste baš prosti brojevi? Zašto ne bilo koja dva velika broja? Odgovor leži u tome da je današnjim računarima veoma lako pomnožiti dva velika prosta broja i naći broj , ali ne postoji način na koji bi se efikasno odradila inverzna operacija kako bi se došlo do faktora i jer to direktno proizilazi iz osnovne teoreme algebre. Ona kaže da se svaki složeni broj, koji je veći od 1, može napisati na tačno jedan način kao proizvod prostih brojeva. Sa malim brojevima je lako, npr. ili , ali kada je dat problem koji izgleda kao , onda je izuzetno teško zaključiti da je i da je . Do današnjeg dana nije osmišljen algoritam koji ovo omogućava i ne preostaje ništa drugo no pokušati sa *brute-force* pretragom (sistematično nabrajanje svih mogućih kandidata za rešavanje problema i proveravanje da li svaki kandidat zadovoljava problem). Ako su brojevi i dovoljno veliki, srednje vreme *brute-force* pretrage može da iznosi nekoliko desetina, pa čak i nekoliko stotina godina, što svakako ide u prilog robusnosti i sigurnosti *RSA* algoritma.

# Zaključak

# Literatura

1. *TCP*, <http://www.rt-rk.uns.ac.rs/predmeti/e2/orm-1-osnovi-računarskih-mreža-1>, jun 2018.
2. *IPv6*,<https://sr.wikipedia.org/sr-el/IPv6>, jun 2018.
3. *RSA*, <https://sr.wikipedia.org/wiki/Enkripcija>, jun 2018
4. *RSA*, <https://simple.wikipedia.org/wiki/RSA_algorithm>, jun 2018