VISOKA POSLOVNA ŠKOLA
STRUKOVNIH STUDIJA
ČAČAK

MAGISTARSKI RAD

Zaštita podataka na IP nivou pod linux OS

Mentor:_____ Student: _____
Profesor: _____ Br.Indeksa: _____

Mesto, mesec, godina

Zaštita podataka na IP nivou pod Linux OS

Xxxxx Xxxxx, Xxxxx Xxxxx
Fakultet za poslovnu informatiku, Univerzitet Singidunum, Beograd

Sadržaj – *U ovom radu se razmatra mogućnost zaštite komunikacija u računarskim mrežama otvorenog tipa na IP nivou pod Linux operativnim sistemom. U dostupnoj stručnoj literaturi postoji mnogo realizacija koje se zasnivaju na standardnim algoritmima i koje su zavisne od proizvođača. Poznato je da profesionalni sistemi zaštite zahtevaju sopstvenu realizaciju, sopstveni algoritam i potpunu kontrolu kriptoloških ključeva. Zbog kompleksnosti protokola i izvornog koda na nižim slojevima računarskih protokola, u našoj zemlji se najčešće razmatraju i realizuju rešenja na aplikativnom nivou. Realizacija na IP nivou bi rasteretila krajnje korisnike od nametanja novih rešenja.*

1. UVOD

Kriptografski mehanizmi zaštite se nalaze u osnovi profesionalnih sistema za zaštitu raznovrsnih informacija i danas predstavljaju najrasprostranjeniji način za ostvarivanje bezbednosti u računarskim mrežama otvorenog tipa. U poslednje vreme je definisan širok dijapazon novih sistema za zaštitu koji se primenjuju za različite sisteme elektronske razmene podataka kao što su zaštićeno slanje datoteka, zaštićeni e-mail servis, sistemi elektronskog plaćanja i sl. Iako se komercijalizacija kriptografskih tehnika veoma brzo širi i zahtevi krajnjih korisnika su takođe sve veći i raznovrsniji. Najbolje karakteristike pokazuju sistemi kod koji se zaštita tajnosti podataka realizuje primenom tradicionalnih simetričnih tehnika, dok se za funkcije autentičnosti, integriteta i neporecivosti transakcija zahteva primena asimetričnih šifarskih sistema sa javnim ključevima – PKI sistemi.

Poznata je činjenica da nivo sigurnosti kod računara i računarskih mreža suštinski zavisi od korektne realizacije, kao i od jednostavnosti primene (instaliranja i korišćenja) konkretnog rešenja. U skladu sa tim, rešenja zaštite koja su potpuno transparentna za krajnje korisnike predstavljaju ideal u savremenom poslovanju. Realizacija zaštite na nižim slojevima računarskog protokola omogućava krajnjim korisnicima da nastave rad na aplikacijama koje dobro poznaju i da se ne opterećuju se strogim bezbednosnim zahtevima u kojima mogu da pogreše. Pored toga, u mnogim slučajevima nije moguće menjati postojeće aplikacije i nadograđivati zaštitne mehanizme. Ono što je najvažnije, rešenja realizovana na nižim slojevima su manje zavisna od realizacija na višim slojevima OSI modela zbog šire standardizacije.

U profesionalnim sistemima zaštite korišćenje sopstvenog algoritma u simetričnim šifarskim sistemima i tajnost simetričnih šifarskih ključeva jesu osnova garancije bezbednosti. Kao dodatna garancija i preduslov za mogućnost realne procene nivoa sigurnosti rešenja jeste i upotreba pouzdanih nosećih softverskih komponenti čiji je izvorni kod dostupan.

U ovom radu je dat primer rešenja bezbednog prenosa podataka neigurnim kanalima (kao što je Internet) koje se realizuje na IP nivou pod Linux operativnim sistemom. a koje ispunjava tri preduslova:

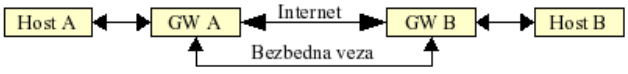
- transparentno je za krajnje korisnike i jednostavno primenljivo,
- koristi sopstveni algoritam za šifrovanje,
- koristi pouzdane noseće komponente sa dostupnim izvornim kodom.

Rešenje zaštite na IP nivou pod Linux operativnim sistemom nudi zadovoljavajuće performanse koje se odnose na primenu sopstvenog algoritma za šifrovanje pod pouzdanim OS [1,5]. Potpuna analiza svih efekata ovakvog rešenja može se izvesti tek nakon dugotrajnog testiranja u raznorodnim mrežnim okruženjima.

2. TRANSPARENTOST I JEDNOSTAVNOST PRIMENE

Posmatraju se dva učesnika iz dve različite lokalne mreže koji u komunikaciji koriste Interent kao standardanu javnu nebezbednu vezu. Zbog transparentnosti i jednostavnosti implementacije, najpogodnije je rešenje koje šifruje podatke na mrežnom sloju (IP) OSI modela. Mana rešenja koje bi bilo realizovano na višim nivoima je jača sprega i zavisnost od softverskih komponenti koje funkcionišu na višem nivou OSI modela (npr. klijentske aplikacije). Mana rešenja koje bi bilo realizovano na nižim nivoima je otežana implementacija i viša cena rešenja.

Sem na nivou OSI modela, postavlja se i pitanje tačaka mreže na kojima se rešenje treba primeniti. Polazeći od pretpostavke da je lokalna mreža (LAN) bezbedna i da se njome mogu prenositi podaci u izvornom (nešifrovanom tj. otvorenom) obliku, tačke na kojima rešenje treba graditi su gateway interfejsi, koji ujedno predstavljaju i granicu između pouzdane (LAN) i nepouzdane (Internet) mreže (Sl. 1).



Sl.1. *Tačke na kojima se instaliraju zaštitni mehanizmi*

Primenom rešenja na gateway interfejsu se, sem transparentnosti, postiže i jednostavnost primene kroz svođenje tj. minimizaciju broja računara na kojima je potrebno instalirati komponente rešenja. Dodatna prednost je i mogućnost administratora sistema da jednostavno određuje u kojim slučajevima će šifrovanje biti korišćeno. Naime, moguće je propuštati saobraćaj koji nije šifrovan, a na osnovu informacija iz zaglavlja paketa vršiti šifrovanje ili dešfrovanje za korisnike koji koriste bezbedan prenosni put [1]. Ovakav prilaz omogućava veliku fleksibilnost sistema,

bez ugrožavanja do tada postojećih komunikacija. Sa druge strane, kako je minimizovan broj računara na kojima se vrši instalacija, administrator može uspešno da kontroliše korektnost primene šifrovanja i dešifrovanja.

3. UPOTREBA SOPSTVENOG ALGORITMA ZA ŠIFROVANJE

Za zaštitu tajnosti podataka standardno se koriste simetrični šifarski sistemi u čijoj osnovi je algoritam za generisanje pseudoslučajnih nizova, koji se inicijalizuje na osnovu tajnih simetričnih ključeva. Pored toga, u postupku kriptološke sinhronizacije generatora pseudoslučajnih nizova bitno je uspešno (tačno) razmeniti posebne ključeve koji se generišu na krajevima za svaku započetu komunikaciju, i eventualno još neke potrebne parametre. Tajnost podataka zaštićenih simetričnim šifarskim sistemima počiva na tajnosti i kvalitetu (slučajnosti) simetričnih šifarskih ključeva. Da bi ovo bilo u potpunosti tačno, neophodno je i da algoritam, koji se koristi za generisanje pseudoslučajnih nizova, zadovolji kriterijume valjanosti [2]. On se projektuje po posebnim kriterijumima, kako bi se sprečili kriptološki napadi usmereni direktno na algoritam.

U komercijalnim proizvodima, dostupnim na tržištu, implementirani su standardni algoritmi kao što su 3DES, AES i sl., sa zadatim dužinama tajnih ključeva koje ne prevazilaze 256. Vrlo često, u konkretnoj aplikaciji moguće je vršiti izbor željenog algoritma. Postojeći standardni algoritmi se uglavnom realizuju modularno, a u procesu kriptološke sinhronizacije zadaje se aktuelni algoritam. U profesionalnim sistemima zahteva se sopstveni algoritam i sopstvena realizacija na softverskoj ili hardverskoj platformi u koju postoji poverenje. Implementacija algoritma je takođe složen posao. Zahteva se da se elementarne strukture algoritma realizuju maksimalno efikasno tj., da njihovo izvršenje traje najkraće moguće. U predloženom rešenju zaštite na IP nivou OSI modela neophodno je izvršiti realizaciju novog algoritma u kernelu operativnog sistema.

4. POUZDANOST NOSEĆIH KOMPONENTI REŠENJA

S obzirom da pouzdanost kompletnog rešenja zavisi od pouzdanosti svake pojedinačne komponente rešenja, da bi se osigurala a zatim procenila pouzdanost kompletnog rešenja potrebno je imati mogućnost provere pouzdanosti svake od komponenti. U tom cilju, neophodno je imati izvorni kod komponenti dostupnim. U ovom rada će se razmatrati Operativni Sistem (OS) kao najdonja noseća komponenta.

Linux operativni sistem predstavlja adekvatnu noseću komponentu za realizaciju funkcija zaštite podataka iz sledećih razloga:

- dostupnost izvornog koda,
- dobre mrežne mogućnosti i performanse,
- firewall je integrisan u kernel,
- IPsec je integrisan u kernel,
- mogućnost realizacije sopstvenog algoritma za šifrovanje kao modula za kernel.

Trenutno postoji veliki broj proizvoda vezanih za sigurnost koji se baziraju na Linux-u,. To su uglavnom distribucije namenjene za zaštitu lokalnih mreža putem firewall-a (SmoothWall, IPCop, Trustix...) mada se Linux takođe javlja i kao integrisani softver u bezbednosnim rešenjima firmi kao što su Innominate AG, secunet Security Networks AG i sl. Neki od razloga zbog kojih se pomenute kompanije odlučuju za Linux kao noseću komponentu svojih rešenja pre nego za MS Windows su:

- mogućnost provere izvornog koda, kao i procene bezbednosti celokupnog rešenja
- mogućnost prilagođavanja izvornog koda sopstvenim potrebama

5. PERFORMANSE

Imajući u vidu da je tačka na kojoj se predlaže implementacija kriptografskih funkcija gatway interfejs, jasno je da se od njega očekuje visoka efikasnost u iskorišćavanju hardverskih resursa. Kroz pomenuti gateway računara prolazi velika količina podataka, a pretpostavka je da veliku većinu, ako ne i sve, treba u što kraćem vremenu šifrovati i proslediti na odredište. Maksimalnu gustinu saobraćaja podataka, koju bi potencijalno trebalo obraditi, najlakše je odrediti preko kapaciteta slabijeg mrežnog linka (pod pretpostavkom da je gateway povezan na dva mrežna linka) na koji je gateway vezan.

Tačan odnos potrebne procesorske snage i bitske brzine podataka koje treba štititi, može se odrediti analizom konkretnog algoritma i testiranjem sa realnim tj. očekivanim saobraćajem podataka. Imajući u vidu visoke performanse Linux operativnog sistema u mrežnom radu, kao i pogodnosti koje nudi implementacija samog IPSec-a i Firewall-a u kernelu, jedino usko grlo može biti sam algoritam. Kompleksni algoritmi, kakvi se zahtevaju u profesionalnim sisteima, zahtevaju značajno vreme za njihovo izvršavanje.

Bitan parametar vrednosti rešenja predstavlja i skalabilnost tj. mogućnost povećanja performansi putem dodatnog hardvera. Povećanje bezbednosti u realizaciji zaštite se može ostvariti realizacijom dodatnog hardvera, na tehnologiji koja omogućuje veliku brzinu izvršavanja kompleksnih algoritama (npr. brzi signal procesori, programabilni hardver - FPGA i sl). Prednosti ovakvog rešenja odnose se na apsolutno poverenje u realizovane funcije šifrovanja i dešifrovanja, uz rasterećenje procesorskog vremena osnovnog računara (u ovom slučaju gateway). Na ovakvim hardverskim modulima za šifrovanje (HSM), pored funkcija šifrovanja i dešifrovanja, moguće je realizovati dodatne hardverske generatore slučajnih nizova, obezbediti siguran prostor za čuvanje šifarskih ključeva, implemetirati podršku za prihvat Smart kartica i sl., što sve značajno podiže ukupnu bezbednost rešenja.

6. IPSEC (IP SECURITY)

Jedno od najpopularnijih rešenja za šifrovanje na mrežnom nivou je svakako IPsec (IP Security) koje je ujedno i standard za obezbeđivanje Internet Protokola (IP). IPsec je set kriptografskih protokola za obezbeđivanje protoka paketa i razmenu ključeva [4]: ESP (Encapsulating Security Payload – omogućuje autentičnost, poverljivost podataka i integritet poruke), AH (Authentication Header – obezbeđuje

autentičnost i integritet poruke ali ne i poverljivost) i IKE (Internet Key Exchange).

S obzirom da IPsec radi na mrežnom sloju OSI modela njime je mnogo lakše omogućiti transparentnost nego široko rasprostranjenim SSL ili TLS sigurnosnim protokolima. Takođe, korišćenjem IPsec rešenja moguće je zaštititi i TCP i UDP bazirane protokole.

Postoji više implementacija IPsec-a (FreeS/WAN, OpenS/WAN, StrongS/WAN...) vezanih za različite operativne sisteme (MS Windows, FreeBSD, NetBSD, OpenBSD, Mac OS X, AIX, Cisco, Linux...). U ovom radu je korišćena implementacija IPsec-a integrisana u kernel Linux operativnog sistema. Autori ove implementacije, Alexey Kuznetsov i David S. Miller, su svoj rad započeli iz osnova, a od kraja 2002. godine se IPsec nalazi kao sastavni deo kernela Linux operativnog sistema verzije 2.6.

Glavni razlozi zbog kojih je ova implementacija IPsec-a dobila prednost nad ostalima su:

- *dostupnost izvornog koda,*
- *integrisanost u kernel obezbeđuje visoke performanse kao i mogućnost korišćenja ostalih komponenti kernela (pre svega algoritama za šifrovanje)*
- *licenca (GPL – General Public Licence)*

7. MODEL REŠENJA

U ovom radu razmatrana je realizacija sopstvenog algoritma na IP nivou OSI modela. Algoritam je realizovan kao modul kernela, na jeziku C, koristeći standardan Crypto API kernela. Funkcije Crypto API-ja u kernelu Linux operativnog sistema su:

- *imealgoritma*_setkey
- *imealgoritma*_encrypt
- *imealgoritma*_decrypt

kao i struktura za rad sa ključevima. Za potrebe testiranja ovakvog pristupa rešavanju problema zaštite primenjen je posebno kreirani algoritam "fbisca". Njegovi osnovni parametri su izabrani i podešeni tako da po broju primenjenih elementarnih struktura, kompleksnosti i dužini tajnog simetričnog ključa bude iznad komercijalno dostupnog AES algoritma. Pri simulaciji algoritma je provereno, a u implementaciji kasnije je izmereno, da je prosečno vreme za generisanje izlaza iz geneatora pseudoslučajnih nizova, kod "fbisca" algoritma veće od prosečnog vremena kod AES algoritma. Na ovaj način je potvrđeno da je moguće integrisati novi algoritam za šifrovanje u sam kernel.

Nakon toga, potrebno je uključiti podršku za IPsec (u vidu modula (m) ili sastavnog dela jezgra (y)):

- CONFIG_INET_AH=y/m
- CONFIG_INET_ESP=y/m
- CONFIG_INET_IPCOMP=y/m

kao i za sopstveni algoritam:

- CONFIG_CRYPTO_FBISCA=y/m

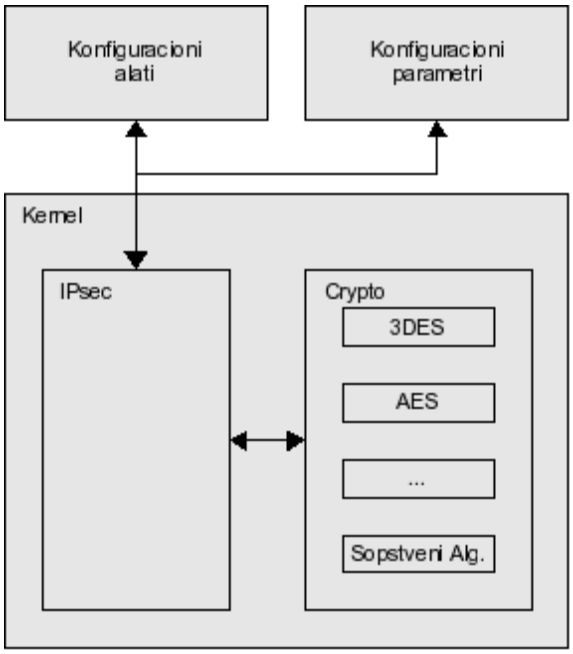
i prevesti izvorni kod. Ovim koracima je dobijeno jezgro operativnog sistema sa integrisanom podrškom za IPsec kao i sopstveni algoritam za šifrovanje.

Međutim, za upotrebu ovakvog sistema neophodno je uključiti dodatne programske pakete za kontrolu jezgra i samog IPsec modula. Jedan od najpopularnijih paketa za ovu namenu je port Kame Project-a paket "IPsec-Tools", namenjen za rad sa IPsec-om implementiranim u kernelu Linux OS-a. Ovaj paket se sastoji od četiri osnovne komponente:

- libipsec - biblioteka PF_KEY implementacije [6]
- setkey - alat za manipulisanje kernelovim SPD (Security Policy Database) i SAD (Security Association Database)
- racoon - Internet Key Exchange (IKE) daemon za automatsko upravljanje ključevima kod IPsec konekcija.
- racoonctl - alat za kontrolu racoon daemon-a

Alternativa paketu "IPsec-Tools" je paket "ISAKMP/Oakley", portovan sa OpenBSD sistema.

Predloženo rešenje je uključivanje svih pomenutih (vezanih za jezgro i sam IPsec) i dodatnih softverskih paketa u sopstvenu Linux distribuciju. S obzirom da je razvoj sopstvene Linux distribucije nepotrebno veliki posao, za osnovu je moguće iskoristiti neku od već postojećih distribucija. Glavni kriterijumi za odabir osnovne distribucije mogu biti: stabilnost, standardnost, dobre mrežne osobine. U skladu sa ovim kriterijumima, predlog za osnovnu distribuciju je "Slackware". Ova distribucija se odlikuje pomenutim osobinama i ima tradiciju od preko 12 godina.



Sl. 2. Model rešenja

Na slici 2 je prikazana šema IPsec implementacije u kernelu, sopstvenog algoritma, konfiguracionih alata i konfiguracionih parametara.

Pod konfiguracionim alatima se podrazumevaju alati za podešavanje konfiguracionih parametara tj. pravila kada će se i koji ključevi koristiti.

8. BEZBEDNOST REŠENJA

Bezbednost ovakvog sistema je veoma važan parametar jer je sistem u stalnom kontaktu sa eksternom, nebezbednom mrežom (npr. Internetom) što znači da je izložen potencijalnim napadima. Posledice ovih napada mogu biti neovlašćen pristup administrativnim funkcijama sistema, otkazivanje rada sistema, krađa ključeva, njihova izmena, brisanje i sl., izmena polisa za šifrovanje podataka, pristup internoj mreži...

Bezbednost sistema zavisi pre svega od pouzdanosti Linux operativnog sistema i IPsec implementacije u njemu ali i od konfiguracije samog kernela i dodatnih softverskih paketa. Najveća opasnost vezana za Linux OS leži u dostupnosti izbornog koda potencijalnim napadačima. Ovo u praksi znači da potencijalni napadač analizom izvornog koda samog Linux OS-a i IPsec implementacije u njemu eventualno može pronaći propust koga autori i korisnici nisu svestni i na osnovu tog propusta, u zavisnosti njegovog tipa, ugroziti stabilnost sistema ili njegovo normalno funkcionisanje, ostvariti neovlašćeni pristup i sl.

Potencijalno rešenje ovog problema bi sadržalo:

- odstranjivanje svih delova (modula) kernela koji nisu neophodni za funkcionisanje opisanog sistema
- namensko korišćenje sistema tj. isključivanje dodatnih funkcionalnosti
- pravilno konfigurisanje sistema i povremenu proveru konfiguracije
- redovno osvežavanje komponenti sistema po preporukama nadležnih autoriteta
- korišćenje IPS/IDS (Intrusion Prevention System / Intrusion Detection System) sistema i sistema koji garantuju nemogućnost modifikacije bilo kog dela sistema bez odgovarajuće provere autentičnosti korisnika
- korišćenje odvojenog računarskog sistema na kome bi se čuvali izveštaji o radu sistema i eventualnim napadima na njega

Takođe, korišćenje standardnih algoritama kao što su AES, DES i sl. koji su pod Linux OS-om dati u izvornom obliku predstavlja sličan problem - eventualne propuste u samim algoritmima potencijalni napadač može iskoristiti snimanjem saobraćaja na koji se tada može gledati kao da je u izvornom, nešifrovanom obliku. Za ovakav tip napada čak nije potreban neovlašćeni pristup gateway sistemima. Korišćenje sopstvenog algoritma rešava ovaj izuzetno ozbiljan problem.

9. ZAKLJUČAK

Opisano rešenje odnosi se na problem bezbednog prenosa podataka nebezbednim kanalima putem šifrovanja podataka sopstvenim algoritmom. Rešenje je realizovano korišćenjem OpenSource tehnologija tako da je moguće proveriti pouzdanost svih komponenti. U radu su prvo analizirani, a zatim prikazani postupci za implementaciju sopstvenog algoritma za šifrovanje u C jeziku korišćenjem Crypto API kernela za Linux operativni sistem. Razmatrano rešenje se oslanja na modularnost standardnih kriptografskih funkcija koje postoje u kernelu. Za osnovu je iskorišćena "Slackware" Linux distribucija.

Predloženo rešenje zaštite podataka na IP nivou OSI modela omogućava uvođenje servisa zaštite u računarskim mrežama bez opterećivanja krajnjih korisnika. Takođe, rešenje pojednostavljuje korišćenje tako da nije potrebna dodatna obuka krajnjih korisnika niti postoji bojazan da rešenje neće biti adekvatno korišćeno.

U ovom radu nije dato rešenje za upravljanje ključevima niti je razmatrana skalabilnosti (poboljšanja performansi putem dodatnog hardvera za šifrovanje). Takođe, opisano rešenje ne rešava problem „nadgledanja saobraćaja" tj. iako je sadržaj komunikacije između mreža A i B nedostupan posmatračima oni još uvek imaju informaciju da je komunikacija obavljena kao i okvirnu informaciju o količini prenesenih podataka.

U radu su detaljno razmatrani različiti aspekti zaštite podataka na IP nivou. Za Linux OS specificirani su postupci i alati za implementaciju sopstvenog algoritma zaštite. Detaljno su razmatrani bezbednosni aspekti ovakvog rešenja. U nastavku ovih aktivnosti neophodno je vršiti detaljnu eksperimentalnu analizu sopstvenih rešenja u raznorodnim mrežnim okruženjima.

LITERATURA

[1] William Stallings, "Cryptography and Network Security", Fourth Edition, Prentice Hall, 2006.

[2] A Menezes at all., "Handbook of Applied Cryptography", CRC Press, 1996.

[3] Daniel de Kok, "Securing IP traffic with IPsec" The Slack World #1, 2005.

[4] Donald Eastlake 3rd "Cryptographic Algorithm Implementation Requirements For ESP And AH",, 2004.

[5] Stephen Kent, Karen Seo, "Security Architecture for the Internet Protocol", 2005.

[6] McDonald D., C. Metz, B. Phan, "PF_KEY Key Management API, Version 2" IETF RFC 2367, 1998.

Abstract: This paper deals with the issue of the protection of computer systems and the possibilities of security precautions related to the communications on the open architecture IP computer network under the Linux operating system. In the existing literature there are numerous designs based on public ciphers depending on the specific product. It is known that professional security systems require their own design, own cipher and complete control over criptographic keys. Due to the complexity of protocols and source codes at lower level of computer protocols, in our country the most frequently implemented solutions are those of application level. The IP level designs would relieve the end users of the pressure of new solutions imposure.

IP SECURITY UNDER LINUX OS

BESPLATNI GOTOVI SEMINARSKI, DIPLOMSKI I MATURSKI RAD.

RADOVI IZ SVIH OBLASTI, POWERPOINT PREZENTACIJE I DRUGI EDUKATIVNI MATERIJALI.

WWW.SEMINARSKIRAD.ORG

WWW.MATURSKIRADOVI.NET

WWW.MATURSKI.NET

WWW.SEMINARSKIRAD.INFO

WWW.MATURSKI.ORG

WWW.ESSAYSX.COM

WWW.FACEBOOK.COM/DIPLOMSKIRADOVI

NA NAŠIM SAJTOVIMA MOŽETE PRONAĆI SVE, BILO DA JE TO SEMINARSKI, DIPLOMSKI ILI MATURSKI RAD, POWERPOINT PREZENTACIJA I DRUGI EDUKATIVNI MATERIJAL. ZA RAZLIKU OD OSTALIH MI VAM PRUŽAMO DA POGLEDATE SVAKI RAD, NjEGOV SADRŽAJ I PRVE TRI STRANE TAKO DA MOŽETE TAČNO DA ODABERETE ONO ŠTO VAM U POTPUNOSTI ODGOVARA. U BAZI SE NALAZE GOTOVI SEMINARSKI, DIPLOMSKI I MATURSKI RADOVI KOJE MOŽETE SKINUTI I UZ NJIHOVU POMOĆ NAPRAVITI JEDINSTVEN I UNIKATAN RAD. AKO U BAZI NE NAĐETE RAD KOJI VAM JE POTREBAN, U SVAKOM MOMENTU MOŽETE NARUČITI DA VAM SE IZRADI NOVI, UNIKATAN SEMINARSKI ILI NEKI DRUGI RAD RAD NA LINKU IZRADA RADOVA. PITANjA I ODGOVORE MOŽETE DOBITI NA NAŠEM FORUMU ILI NA MATURSKIRADOVI.NET@GMAIL.COM