VISOKA POSLOVNA ŠKOLA
STRUKOVNIH STUDIJA
ČAČAK

MAGISTARSKI RAD

Ipsec - analiza uticaja algoritma za g̈ifrovanje na saobraĺaj u lan mreǵama

Mentor:_____ Student: _____

Profesor: _____ Br.Indeksa: _____

Mesto, mesec, godina

IPsec – analiza uticaja algoritma za šifrovanje na saobraćaj u LAN mrežama

Xxxxx Xxxx, Xxxxx Xxxxx

***Sadržaj* — U ovom radu analiziran je uticaj algoritama za šifrovanje na opterećenost procesora umreženih računara pri visokim bitskim brzinama prenosa podataka. Analiza je usmerena na izmenu vremenske komponente za izvršenje jednog algoritma. Korišćena je realizaciju IPsec-a pod Linux operativnim sistemom, na računarima sa AMD i Intel procesorima. Tablearno i grafički dati su rezulati kod primene DES, AES i modifikovanog AES algoritma. Pokazano je da softverska realizacija algoritama za šifrovanje ima svojih vremenskih ograničenja i to za gigabitne komunikacije.**

***Ključne reči* — 3DES, AES, AH, algoritam za šifrovanje, analiza performansi, bezbedna komunikacija, Crypto API, ESP, IPsec, Linux, računarske mreže, zaštita.**

I. UVOD

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.

Jedan od posrednih uslova za uspešnost rešenja predstavlja i njegova sveobuhvatnost kao i jednostavnost upotrebe. Sveobuhvatnost rešenja se može bazirati na nivou OSI modela na kome je ono primenjeno. Realizacija rešenja na previše niskom nivou može stvoriti nekompatibilnost sa postojećim računarskim mrežama, dok realizacija na previše visokom nivou može ograničiti skup komunikacija koje rešenje obuhvata kao i dodatno usložiti upotrebu. U skladu sa tim, IP nivo se postavlja kao ultimativno rešenje.

IPsec predstavlja standardno rešenje za bezbednost komunikacija baziranih na IP protokolu. Mogućnosti šifrovanja i utvrđivanja autentičnosti učesnika u komunikaciji, rad u maskiranim mrežama, korišćenje na različitim operativnim sistemima su samo neke od karakteristika ovog popularnog rešenja. Podrška za popularne algoritme (AES, 3DES...) i otvorenost standarda su osnova za proširivanje rešenja. Inicijalni dizajn na IPv6 protokolu je garancija buduće kompatibilnosti.

Aleksandar Jevremović, Fakultet za poslovnu informatiku, Univerzitet Singidunum, Danijelova 32 Beograd; telefon: 381-11-3093238; e-mail: ajevremovic@singidunum. ac.yu

Mladen Veinović, Fakultet za poslovnu informatiku, Univerzitet Singidunum, Danijelova 32 Beograd; telefon: 381-11-3093227; e-mail: mveinovic@singidunum. ac.yu

U radu [7] obrađena je IPsec implementacija na Linux operativnom sistemu verzije 2.6., kao i mogućnosti koje nudi dostupnost izvornog koda, pre svega proširenje baze algoritama za šifrovanje sopstvenim algoritmom. U ovom radu, fokus je stavljen na analizu performansi obrađenog rešenja i analizu mogućnosti procesora PC računara na megabitnim i gigabitnim komunikacionim kanalima.

II. LINUX/IPSEC PLATFORMA

Kao što je rečeno u delu I postoji više realizacija IPsec-a na različitim operativnim sistemima. Izvorni kod nekih od realizacija je dostupan i/ili postoji mogućnost proširenja dok su neke realizacije potpuno zatvorene. Za potrebe ovog rada (kao i u radu [7]) iskorišćena je IPsec realizacija u jezgru Linux operativnog sistema. Postoji više razloga za ovakav izbor:

1. Realizacija na nivou kernela nudi efikasan pristup (bliskim) sistemskim resursima što je jedan od preduslova za visoke performanse celokupnog sistema. Dokaz opravdanosti ovakvog pristupa je i *netfilter* firewall, takođe realizovan u samom kernelu, čije su performanse i nivo bezbednosti koji nudi na veoma visokom nivou.
2. Celokupan kod Linux operativnog sistema je javno dostupan (uključujući i sam IPsec i algoritme) što daje mogućnost:
   a) provere ispravnosti/bezbednosti komponenti koje će biti uključene,
   b) izmenu neodgovarajućih komponenti,
   c) dodavanja sopstvenih komponenti,
   d) testiranja i verifikacije implementiranog rešenja.
3. Linux je modularan operativni sistem što omogućava da se celokupna bezbednost računara (na kojima je primenjeno opisano rešenje) poveća isključivanjem svih podrški u jezgru koje nisu potrebne.
4. Performanse i mogućnosti (pre svega u radu na mreži) Linux operativnog sistema u potpunosti odgovaraju zahtevima koji se postavljaju pred jedan sistem čija je uloga bezbedno povezivanje velikog broja internih klijenata sa udaljenom mrežom putem brzih komunikacionih kanala.

Stavka 2-c prethodne liste je od suštinske važnosti u profesionalnim sistemima zaštite, jer omogućava primenu sopstvenog algoritma u procesu šifrovanja. Dalje, primena Linux operativnog sistema obezbeđuje mogućnost provere izvornog koda, a time i uslove za procenu bezbednosti celokupnog rešenja.

III. SOPSTVENI ALGORITAM

Mogućnost korišćenja sopstvenog algoritma u određenom gotovom rešenju podrazumeva adekvatan API (tj. mogućnost proširenja rešenja sopstvenim modulima) ili/i dostupnost izvornog koda rešenja. Kao što je rečeno u delu 2 (Linux/IPsec platforma) kompletan izvorni kod Linux operativnog sistema, IPsec implementacije u njemu i uključenih algoritama je dostupan.

U radu [7] korišćen je Crypto API u kome je proširen skupa algoritama za šifrovanje u kernelu operativnog sistema. U ovom radu je iskorišćena druga mogućnost tj. modifikovan je izvorni kod AES algoritma. Mane ovakvog pristupa su:

- mogućnost nasleđivanja eventualnih nedostataka AES algoritma
- nemogućnost paralelnog korišćenja AES algoritma i njegove modifikovane varijante na istom sistemu

Osnovni razlozi za ovakav pristup su:

- minimalno područje izmena za dobijanje željene funkcionalnosti algoritma
- cilj da se rezultati dobijeni izmenjenim algoritmom uporede sa rezultatima originalnog AES algoritma.

Sama zamena algoritma je izvršena zamenom fajla sa izvornim kodom algoritma, aes.c u crypto direktorijumu izvornog koda jezgra Linux operativnog sistema. Nakon zamene izvornog koda izvršeno je ponovno prevođenje fajla. S obzirom da je u konfiguraciji jezgra AES algoritam podešen kao modul, nije bilo potrebe za ponovnim prevođenjem osnovne slike jezgra.

U izmenu algoritma spada usporavanje algoritma preko bloka naredbi čiji je cilj oduzimanje procesorskog vremena. Izmena je primenjena na oba sistema koja su korišćena u eksperimentu. S obzirom na to da je cilj ovog rada analiza performansi algoritama nije bilo potrebe za ozbiljnijom izmenom. Takođe, dobijeni algoritam je kompatibilan sa originalnom varijantom AES-a.

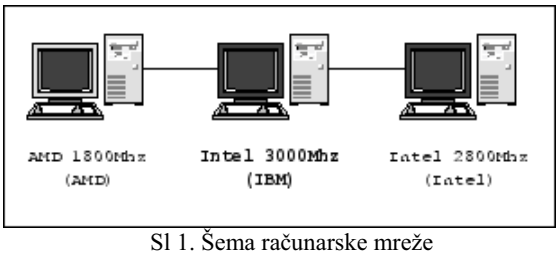
Svaki algoritam za šifrovanje može se okarakterisati sa dva bitna svojstva: zahtevom za memorijskim resursima i vremenom za njegovo izvršavanje. Memorijski resursi na savremenim računarima su ogromni, tako da njihova izmena nije od interesa. Ključni su vremenski resursi, tj vreme potrebno za jedan "okret" algoritma. Algoritmi predstavljaju skup međusobno povezanih elementarnih struktura, za čije izvršavanje se troši značajno procesorsko vreme. Cilj ovog rada je bio da se proveri koliki je uticaj softverskih realizacija algortama za šifrovanje na opterećenost procesora. Upravo iz ovog razloga, analiziran je uticaj vremenske komponente za izvršavanje pojedinih algoritama. Sama struktura algoritma nije bila od interesa jer u profesionalnim sistemima projektovanje algoritma realizuju specijalne službe.

Pored memorijskih i vremenskih resursa jednog algoritma od izuzetne važnosti je i korektnost realizacije tj. mogućnost testiranja i verifikacije realizovanog rešenja. Iscrpnom eksperimentalnom analizom provereno je da su sve izmene u standardnom AES algoritmu korektno realizovane, što je pokazatelj da je i algoritam i operativni sistem računara potpuno pod kontrolom. U daljem delu ovog rada su prikazani rezultati dobijeni za AES algoritam, 3DES algoritam i izmenjeni AES algoritam. Testiranje sa originalnim AES algoritmom je izvršeno pre modifikacije algoritma.

IV. EKSPERIMENT

Za potrebe eksperimenta korišćena su tri međusobno umrežena računara, dva za primenu IPsec rešenja a jedan za ulogu bridža tj. snimanje saobraćaja (slika 1). Imena u zagradama na slici 1. predstavljaju simboličke nazive koji će biti korišćeni u daljem tekstu. Detaljnije hardverske karakteristike prikazane su u tabeli 1.

Uloga AMD i Intel računara je primena IPsec rešenja za šifrovanje a IBM računara snimanje komunikacije i provera rezultata šifrovanja.



Sl 1. Šema računarske mreže korišćene u eksperimentu

TABELA 1: HARDVERSKE KARAKTERISTIKE RAČUNARA KORIŠĆENIH U EKSPERIMENTU

AMD	
Procesor:	AMD Sempron(TM) 2200+ 1800MHz 256KB cache
RAM:	256MB
Mrežna kartica:	Realtek RTL-8169 Gigabit Ethernet
Intel	
Procesor:	Intel(R) Pentium(R) D 2.8GHz 1024KB cache
RAM:	4096MB
Mrežna kartica:	NetLink BCM5789 Gigabit Ethernet
IBM	
Procesor:	2 x Intel(R) Xeon(TM) CPU 2 x 3.00GHz 2 x 2048KB cache
RAM:	4096MB
Mrežna kartica:	2 x NetXtreme BCM5721 Gigabit Ethernet

Na sva tri računara instaliran je Slackware Linux 10.2

sa kernelom 2.6.17.8. Na AMD i Intel računaru je uključena podrška za IPsec:

- CONFIG_NET_KEY = Y
- CONFIG_INET_AH = Y
- CONFIG_INET_ESP = Y

kao i odgovarajuće kripto-algoritme:

- CONFIG_CRYPTO_HMAC = Y
- CONFIG_CRYPTO_MD5 = Y
- CONFIG_CRYPTO_SHA1 = Y
- CONFIG_CRYPTO_DES = Y
- CONFIG_CRYPTO_AES = Y

dok je na IBM računaru uključen modul za bridž:

- CONFIG_BRIDGE = Y

Od dodatnog softvera na AMD i Intel računarima je korišćen program netperf, a na IBM računaru program ethereal.

Program netperf omogućava izvršavanje različitih testova vezanih za mrežu. Jedna od glavnih osobina ovog softvera je to što je realizovan u vidu klijentske i serverske komponente, tako da omogućava praćenje željenih parametara i na klijentskoj i na serverskoj strani, istovremeno. Rezultati testiranja performansi mreže u ovom radu dobijeni su uz pomoć pomenutog programa.

Program ethereal omogućava snimanje mrežnog saobraćaja koji prolazi kroz računar na kome je instaliran i olakšava analizu razdvajajući saobraćaj po nivoima protokola. Ovaj softver je u eksperimentu korišćen za kontrolu saobraćaja između AMD i Intel računara tj. proveru da li se šifrovanje podataka na njima odvija kako je planirano.

Nakon postavljanja eksperimentalnog okruženja pristupile se merenju mrežnih performansi sa sledećim karakteristikama:

- korišćen je desetosekundni TCP stream generisan pomoću netperf softvera
- merenje je izvršeno po tri puta za svaki od algoritama (AES, 3DES i modifikovani AES, mAES) kao i za prenos bez šifrovanja (bez korišćenja IPsec-a)
- svako merenje je vršeno po dva puta tj. u dva smera (od AMD-a ka Intel-u i obrnuto)
- kod svih šifrovanih komunikacija su korišćeni i AH (Authentication Header) i ESP (Encapsulated Security Payload)
- za sva merenja je korišćena ista hardverska i mrežna platforma

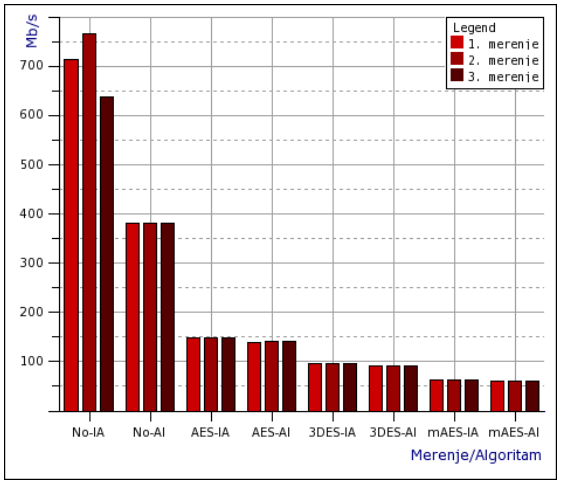
Pri svakom od merenja beleženi su sledeći parametri:

- ostvarena brzina protoka podataka
- opterećenje centralnog procesora pošiljaoca
- opterećenje centralnog procesora primaoca

Za sve algoritme su korišćeni isti ključevi dužine 128 bita (za AH) i 192 bita (za ESP). Dobijeni rezultati predstavljeni su u delu V. Analiza rezultata.

V. Analiza rezultata

Rezultati merenja su prikazani na slici 2. (dijagram ostvarenih brzina protoka) i u tabeli 2.



Sl 2. Dijagram sa ostvarenim brzinama protoka po algoritmu

Na slici 2. se vidi pad brzine prenosa podataka pri korišćenju zahtevnijih algoritama za šifrovanje. Imajući u vidu da je za sva merenja korišćena ista hardverska platforma i isti komunikacioni kanal (iste propusne moći) jasno je da razlog usporenja leži u opterećenju procesora učesnika u komunikaciji tj. njihovoj mogućnosti da u jedinici vremena šifruju/dešifruju određenu količinu podataka.

Tabela 2: Rezultati merenja.

Ostvarena brzina (Mb/s)	CPU opterećenje pošiljaoca (%)	CPU opterećenje primaoca (%)
No enc. (Intel -> AMD)		
712.41	14.52	77.52
765.25	15.06	84.31
636.59	12.73	69.63
No enc. (AMD -> Intel)		
381.11	42.56	22.38
380.91	41.86	21.33
380.96	42.17	22.34
AES (Intel -> AMD)		
147.99	36.22	99.90
148.15	36.18	99.90
148.03	36.25	99.90
AES (AMD -> Intel)		
140.05	99.90	47.93
140.47	99.90	47.89
140.25	99.90	47.82

3DES (Intel -> AMD)		
96.25	35.93	99.90
95.70	35.82	99.90
95.51	35.92	99.90
3DES (AMD -> Intel)		
91.68	99.90	40.99
91.55	99.90	40.01
91.57	99.90	41.23
mAES (Intel -> AMD)		
63.72	30.83	99.90
63.75	31.00	99.90
63.74	30.89	99.90
mAES (AMD -> Intel)		
61.33	99.90	37.22
61.44	99.90	36.28
61.40	99.90	36.07

U tabeli 2. su brojčano date vrednosti prikazane na dijagramu slike 2. kao i opterećenje procesora (u procentima) učesnika u komunikaciji. S obzirom na to da je opterećenje AMD procesora pri korišćenju svakog od algoritama bilo na maksimumu (99,9% + 0,01% za sistemske procese) to jasno ukazuje na usko grlo ovih komunikacija. Takođe, moguće je predvideti 2-3 puta veću brzinu korišćenjem snažnijeg procesora kakav je u Intel računaru.

Napomena: U ovom radu nije rađeno poređenje mogućnosti procesora kompanija Intel i AMD. Skromnije mogućnosti AMD procesora su svakako očekivane jer je taj procesor znatno stariji od korišćenog Intel procesora, radi na nižoj frekvenciji i ima manju količinu keš memorije. U eksperimentu su namerno korišćeni sistemi različitih mogućnosti da bi se što bolje procenilo opterećenje šifrovanjem velike količine podataka u što kraćem vremenskom periodu.

VI. Zaključak

Rezultati ovog rada pokazuju da performanse današnjih PC računara nisu dovoljne za potpuno iskorišćenje mogućnosti gigabitnih komunikacionih kanala u slučaju primene algoritama za šifrovanje na opisanoj platformi. Dobijeni eksperimentalni rezultati ukazuju na potrebu dodatnog hardvera za šifrovanje umesto softverskog algoritma i na taj način povećanje performansi do nivoa gigabitnih i bržih komunikacionih kanala.

Ipak, gigabitni komunikacioni kanali van lokalnih mreža (koje i nisu ciljno područje za zaštitu jer se u većini slučajeva njihovi komunikacioni kanali smatraju bezbednim) su retkost. Daleko češća situacija je kada je propusna moć nebezbednog kanala nekoliko stotina puta manja pa je treba što bolje iskoristiti uz pomoć kompresije podataka pre šifrovanja, što predstavlja još jedan od pravaca daljih istraživanja.

Ovim radom, takođe, nije obuhvaćen problem razmene i upravljanja ključevima, što će biti predmet daljih istraživanja.

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.

[7] Aleksandar Jevremović, Mladen Veinović, “Zaštita podataka na IP nivou pod Linux OS”, ETRAN, 2006. Beograd

Abstract

In this paper influence of cryptographic algorithm on CPU load of network computers on high bit streams is analyzed. Analyze is focused on changing of time component of the cryptographic algorithm. Linux operating system IPsec implementation is used on AMD and Intel central processing units. Results for DES, AES and modified AES are given as tables and diagrams. It's shown that software cryptographic algorithm is limited, especially for gigabit communication channels.

IPSEC – ANALYZING INFLUENCE OF CRYPTOGRAPHIC ALGORITHM ON LAN NETWORKS TRAFFIC

Xxxxx Xxxxxxx, Xxxxx Xxxx

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