Performanse kriptovanja na sistemima datoteka

Dragoljub Pilipović, Dejan Stjepanović

***Sadržaj* — U današnjem svetu sveopšte povezanosti podaci lako postaju informacije, te je sigurnost podataka važno implementirati. Enkripcija je nezaobilazno sredstvo zaštite, te će stoga u ovom radu biti prikazane performanse encrypting datotečnog sistema na tipičnom ličnom računaru.**

***Ključne reči* — EFS, EncFS, enkripcija, performanse, sigurnost, sistemi datoteka.**

I. Uvod

SVRHA ovog rada je prikaz pojedinačnih i komparacija performansi kriptovanja između najpopularnijih današnjih operativnih sistema: Windows i Linux. Rad uključuje komparaciju performansi sa podrazumevanim vrednostima posle instalacije navedenih operativnih sistema na tipičnom ličnom računaru. Tipičan PC treba da bude najrasprostranjeniji računar u upotrebi i da bude lako dostupan za kupovinu, oboje u trenutku pisanja rada. Mislimo da je dobar kao reprezentacija prenosivi računar (laptop) sa Intel-ovim Celeron M procesorom, radnom memorijom od 512MB, Intel-ovim skupom osnovnih čipova i integrisanom grafikom. Kao jedinicu masovne stalne memorije isti poseduje 120GB tvrdi disk sa 5400 obrtaja u minuti i keš memorijom od 8MB.

Takođe treba da ima popularan operativni sistem. Mislimo da je to svakako MS Windows XP, ali mu se kao alternativa suprostavlja, ne sledeća iteracija iz iste firme, već operativni sistem otvorenog koda i besplatan kao što je Linux firme Ubuntu poslednje dostupne verzije 8.04.

Performanse su izmerene pomoću sopstvenih benchmark test programa, koji bi trebalo da odražavaju osnovne operacije sa kriptovanim datotekama: kopiranje u kriptovani direktorijum i kopiranja iz njega.

Struktura rada se sastoji od opisa Windows platforme i konstrukcije i izvođenja testova, te istog opisa za alternativni Linux, posle čega idu rezultati prikazani tabelarno i grafički, kao i pojedinačno i uporedno. U zaključku je data kratka diskusija dobijenih rezultata.

II. Windows platforma

A. *Opis platforme*

New Technology File System (NTFS) predstavlja sistem datoteka opšte namene koji je uobičajen na Windows familiji operativnih sistema američke firme Majkrosoft. Njegovo prvo pojavljivanje je vezano uz Windows NT 3.1 iz 1993. godine. Verzije su vezane za pojedine inkarnacije operativnih sistema, te je danas aktuelan NTFS sa verzijom 5.1 [1].

Tako je NTFS visokoperformansni i samoobnovljivi sistem datoteka sa najvećim volumenom od 256 TiB - 64 KiB i najvećom mogućom datotekom od 16 TiB - 64 KiB [2]. Tačna specifikacija ovog sistema datoteka nije poznata, jer predstavlja komercijalnu tajnu.

Od verzije 5.0, NTFS ima mogućnost disk enkripcije objekata sistema datoteka putem Encrypting File System-a (EFS) [3].

Za uključivanje enkripcije neke datoteke ili direktorijuma potrebno je uraditi jednu od sledećih akcija:

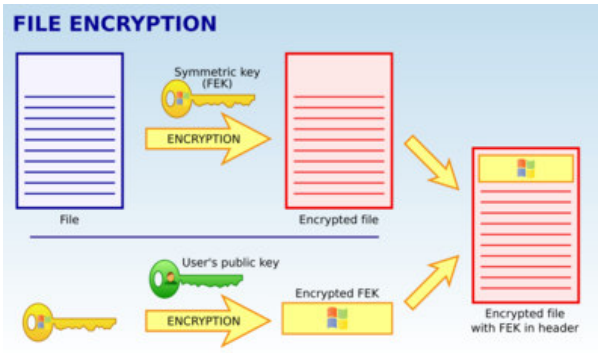
- U grafičkom modu za izabrani objekat u njegovim svojstvima na dijalogu Advanced Attributes izabrati opciju Encrypt contents to secure data.
- Dodati neki objekat u već enkriptovan direktorijum.
- U konzolnom režimu koristiti naredbu cipher.exe sa odgovarajućim parametrima.

Enkripcija se isključuje na isti način, ali u suprotnom smeru.

EFS koristi kombinaciju simetričnog i asimetričnog načina šifrovanja. Simetrični ključ šifrovanja (FEK, File Encryption Key) se koristi za same podatke odnosno za pojedinačne datoteke. Par javnog i privatnog RSA ključa se koristi da bi zaštitio simetrični ključ [2].

Proces enkripcije jedne datoteke se sastoji od sledećih koraka (sl. 1.):

1. Operativni sistem pravi jedinstveni simetrični ključ FEK.
2. Koristeći FEK šifrira se polazna datoteka.
3. Korisnikov javni ključ će biti upotrebljen za šifrovanje FEK-a.
4. Konačna šifrovana datoteka se sastoji od šifrovanog FEK-a i šifrovane polazne datoteke.



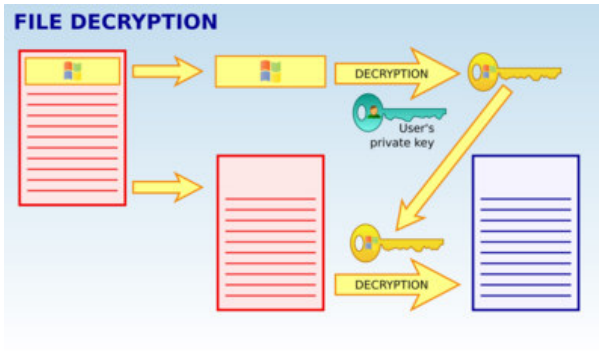
Sl. 1. Proces EFS enkripcije datoteke [2]

Dragoljub Pilipović, Slobomir P Univerzitet, Bijeljina, Republika Srpska, Bosna i Hercegovina (e-mail: dragoljub.pilipovic@gmail.com).

Dejan Stjepanović, Administrativna služba Grada Banja Luka, Republika Srpska, Bosna i Hercegovina (e-mail: dejan.stjepanovic@gmail.com)

Obrnut proces za jednu enkriptovanu datoteku se sastoji od sledećeg (sl. 2.):

1. Izdvajaju se šifrovani FEK i šifrovani podaci datoteke.
2. Pomoći korisnikovog tajnog ključa se izvodi dešifrovanje simetričnog ključa.
3. Sada se FEK koristi za simetrično dešifrovanje da bi se dobila polazna datoteka.



Sl. 2. Proces EFS dekripcije datoteke [2]

U EFS-u se koriste razni kriptografski algoritmi i tehnike, poput DES-X, 3DES, AES, RSA, RC4 i druge jednosmerne hash funkcije.

NTFS 5.0 u Windows 2000 operativnom sistemu koristi jedino DES-X kao simetrični algoritam, NTFS 5.1 kod Windows XP Proffesional-a alternativno može da koristi 3DES, dok je ista verzija ako ima Service Pack 1 instaliran, ili veći, sposobna da koristi kao treći algoritam i AES-256 (kao i sve Server 2003 i Vista ne-kućne verzije).

EFS koristi bazu podataka Registry da odluči koji će simetrični algoritam koristiti od raspoloživih [2].

Proces obnavljanja odnosno oporavka (recovery) je sličan dekripciji, osim što koristi privatni ključ recovery agenta da bi se dekriptovao FEK u DRF, ne u DDF polju. Korisnički nalog koji je vezan za sertifikat agenta za oporavak će izvršiti dekriptovanje datoteke.

Egzistencija agenta za oporavak zavisi od verzije operativnog sistema i njihovog okruženja. Tako na samostalnom Windows XP Professional sistemu ne postoji podrazumevani agent po instaliranju sistema od nule, na Windows Server 2003 on postoji, dok je za članove domena podrazumevani onaj koji je definisan grupnim politikama domena.

B. Opis testa

Preko paralelne veze (PATA) je priključen spomenuti tvrdi disk firme Western Digital model WD1200BEVE. Na logičku particiju veličine 9,5GB je instaliran MS Windows XP Professional sa SP2 (Service Pack 2), te je ostalo slobodnog prostora oko 8GB. Integrisana grafička karta je uzela od ukupne radne memorije 16MB, što je podešeno u BIOS-u laptopa. Na sistemu je bio prijavljen samo jedan korisnik. Testovi su se izvodili u korenu sistema datoteka.

Test podaci su podeljeni u dva paketa. Prvi paket (packet 1) je sadržao jednu .avi datoteku veličine 700MB sa video materijalom kompresovanim u MPEG4/DivX tehnici. Drugi paket (packet 2), veličine 225MB, se sastojao od velikog broja manjih datoteka i to: 3.218 datoteka i 162 direktorijuma. U njemu su se najčešće nalazili sledeći formati: html, txt, c, h, cpp, java, css, jpeg, gif, doc, pdf, zip, rar i jar. Ova dva paketa su izabrana kao reprezent vrsta podataka i njihove strukture koje se mogu najčešće naći na tipičnom ličnom računaru.

Napravljena su dva foldera: „kript“ sa postavljenim enkripcionim bitom i „izvor“ bez tog bita. Testovi su se sastojali iz tri dela:

1. obično kopiranje u „izvor“ folder,
2. kopiranje iz „izvor“ foldera u „kript“ folder i
3. kopiranje iz „kript“ foldera u „izvor“ folder.

Za svaki deo je napravljena posebna batch datoteka, koje su veoma slične. Npr, za 2. ona izgleda ovako:

```
echo |time > rezultati.txt
xcopy izvor kript /e /q
echo |time >> rezultati.txt
```

U prvoj liniji se koristi spajanje dve naredbe: naredba echo šalje prazan karakter i znak za novi red naredbi time koja ispisuje tekuće sistemsko vreme i pita za novo vreme. Novo vreme neće biti postavljeno, što je dobijeno pogodnim izborom parametra echo naredbe. Umesto da se prikaže na standardnom izlazu, sav izlaz iz obe naredbe će biti preusmeren u novokreiranu datoteku rezultati.txt. Nešto slično će se dogoditi u trećem redu, uz razliku da će izlaz biti nadopunjen u postojeću rezutalti.txt datoteku. Ove dve linije služe za beleženje početka i kraja operacije kopiranja i one su iste u svim batch datotekama.

U liniji broj dva se nalazi naredba za kopiranje u kojoj se prema potrebi menjaju parametri. Prvi parametar je folder iz kog se kopira u folder koji je naveden kao drugi argument. Dodatak /e govori da se kopira cela struktura podfolera, a dodatak /q da nema štampanja izlaza na ekran. Ako je linija broj dva privremeno isključena u izvršavanju, vremenska razlika između prvog i trećeg reda je konstantna i iznosi 0,07 sekundi.

Svaki deo testa je pokrenut tri puta, te je nađena njihova srednja vrednost. Rezultati su ručno vađeni iz rezultati.txt fajla i kasnije obrađivani u programu za tabelarna izračunavanja. Sva izvršavanja su pokretana iz komandnog prozora. Između svakog pojedinačnog izvršavanja batch datoteke, pokrenuti su zahtevniji programi (u smislu zauzeća radne memorije) da bi se donekle ublažio efekat keširanja disk sadržaja.

III. LINUX PLATFORMA

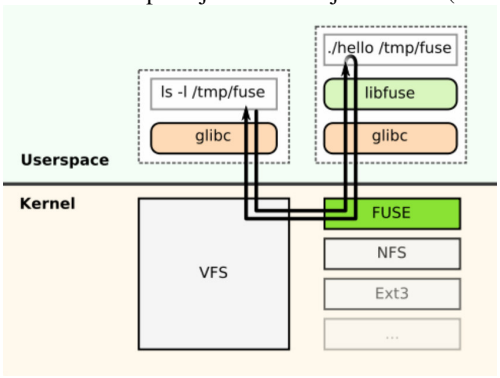
A. Opis platforme

Linux predstavlja savremen, sofisticiran i moćan operativni sistem otvorenog koda. Novije verzije Linux jezgra uključuju podršku za visoko performansne journaling sisteme datoteka, poput ext3, ReiserFS, JFS i XFS [4].

Podrazumevani sistem datoteka u većini Linux distribucija je ext3, što je skraćenica od Third Extended File System. Njega je autor Stiven Tvidi, doktor tehničkih nauka i aktivan programer u zajednici posvećenoj otvorenom kodu, predstavio 1999. godine [3].

Sistem ext3 je kompatibilan sa svojim predhodnikom, ext2 sistemom datoteka, i predstavlja njegovu nadogradnju dnevničkim (log, journal) slojem [5]. Njegova prednost je što daje umerene i ujednačene performanse; uz to je jednostavan za implementaciju i široko dostupan. Mane proizilaze iz činjenice da je projektovan da zadrži potpunu kompatibilnost sa ext2 sistemom. Najveća moguća datoteka je 2 TiB, dok se granica pojedinačnog volumena nalazi na 16 TiB.

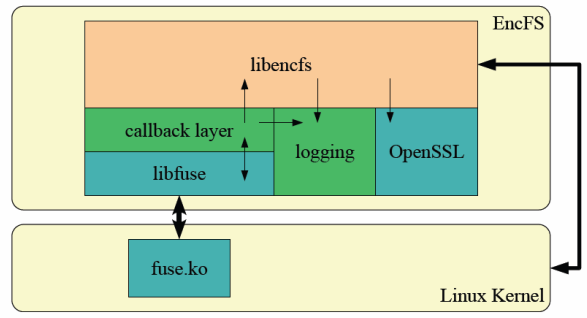
EncFS predstavlja kriptovani virtuelni sistem datoteka koji je pokrenut i izvršava se u korisničkom režimu rada UNIX-olikih operativnih sistema. Za te svrhe koristi FUSE (Filesystem in Userspace) modul. FUSE je programski modul jezgra, koji dozvoljava neprivilegovanim korisnicima da kreiraju svoj lični sistem datoteka bez menjanja samog jezgra operativnog sistema. Ovaj modul je svojevrsni most ka postojećem interfejsu kernela (sl. 3.)



Sl. 3. Prikaz komunikacije sa FUSE modulom

FUSE modul je posebno upotrebljiv pri projektovanju virtuelnih sistema datoteka. Oni nisu namenjeni prevashodno čuvanju i čitanju podataka, kao što su to tradicionalni datotečni sistemi, već deluju kao sloj za drugačiji pogled ili transformaciju postojećih zapisanih podataka. Tako svaki podatak dostupan kroz FUSE implementaciju se može prikazati kao samostalan sistem datoteka.

EncFS (Encrypted File System) je razvijen i dalje se održava od strane Valijent Goga [6], koji ga je prvi put predstavio 2003. godine. Izabran je za ovaj rad, jer je donekle sličan EFS-u. Transparentno za korisnika kriptuje određeni direktorijum i sve objekte što su u njemu. Koristi OpenSSL kao dobavljač kripto algoritama, najčešće AES i BlowFish sa više različitih dužina ključa (sl. 4.)



Sl. 4. Prikaz rada i strukture EncFS sistema

Potrebna su dva direktorijuma za pravilan rad. Prvi sadrži originalne podatke koji su kriptovani i na taj način zaštićeni. Drugi direktorijum je tačka montiranje (mount point) preko koga se sadržaj prvog direktorijuma vidi u jasnom obliku (clear text). Sa stanovišta korisnika računara, posle inicijalnog montiranja sistema datoteka, sve se akcije odvijaju u drugom direktorijumu.

EncFS virtuelni sloj deli sva ograničenja datotečnog sistema nad kojim je implementiran. Razlika u odnosu na opisani EFS je ta da su imena datoteka u kriptovanom direktorijum takođe kriptovana. Sva ostale informacije, poput dozvola i datuma za neku datoteku, su vidljive i identične originalnim. Druga razlika se ogleda u nepostojanju mehanizma oporavka, jer bez unete lozinke pri kreiranju fajl sistema nije moguće doći do dekriptovanih podataka. Lozinkom je zaštićen slučajno generisani ključ (volume key), različit za svaki fajl sistem, a nalazi se u korenu prvog direktorijuma u tekstualnoj datoteci .encfs6.xml.

Za instalaciju EncFS sistema je prvo potrebno proverite da li postoji učitan FUSE u jezgro (cat /proc/filesystems | grep fuse). Napraviti dva direktorijuma (prvi neka je .kript, a drugi neka se zove kript, oba unutar home direktorijuma). Posle toga ide montiranje fajl sistema sa encfs ~/.kript ~/kript. Tako će prvi biti skriven i enkriptovan, a drugi će biti dostupan onome ko zna lozinku i ko ima odgovarajuće pristupne dozvole (rwx). Putanje do direktorijuma moraju biti apsolutne. Ako je ovo prvi put da se pokreće encfs sa ovim parametrima, biće postavljeno više konfiguracionih pitanja, od kojih je najvažnije ono o lozinci. Ako je konfiguracija ranije izvršena, posle ukucane ispravne lozinke, biće mount-ovan novi sistem datoteka i može se koristiti na uobičajen način.

B. Opis testa

Na logičku particiju veličine 6,5GB sa mount point-om / je instaliran Ubuntu Linux verzije 8.04 sa kernelom 2.6.24-16-generic, a za swap particiju je dodeljen prostor veličine 1,8GB. Na osnovnoj particiji je ostalo slobodno 4 GB. Postojao je jedan prijavljen korisnik na sistem. Instaliran je EncFS verzije 1.4.2-2 iz .deb paketa, sa zavisnim paketima libboost-serialization i librlog1c2a. Napravljena su dva potrebna direktorijuma, plus jedan nekriptovan („izvor“) i montiran novi fajl sistem. Koristi se podrazumevani algoritam AES sa dužinom ključa od 192 bita.

Paketi za testiranje su identični. Takođe testovi su ostali isti, ali je realizacija jednostavnija zbog postojanja komande time. Na primer, deo testa 2 je realizovan sledećom naredbom: time cp izvor/* kript –r.

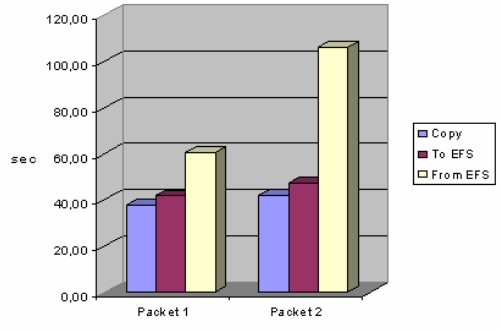
Komanda time meri vreme potrebno da se izvrši naredba koja je navedena kao njen parametar, u ovom slučaju kopiranje svih objekata rekurzivno iz izvora u kript. Kao izlaz se dobijaju tri vremena: stvarno, korisničko i sistemsko. Kao relevantno za naše testove je uzeto stvarno (real) vreme.

Svaki deo testa je pokrenut tri puta, te je nađena njihova srednja vrednost. Rezultati su ručno vađeni iz terminal prozora i kasnije obrađivani u programu za tabelarna izračunavanja. Sva izvršavanja su pokretana iz konzolnog prozora. Između svakog pojedinačnog izvršavanja skript datoteke su pokrenuti zahtevniji programi (u smislu zauzeća radne memorije), da bi se donekle ublažio efekat keširanja disk sadržaja.

IV. REZULTATI TESTOVA

TABELA 1: REZULTATI ZA WINDOWS PLATFORMU

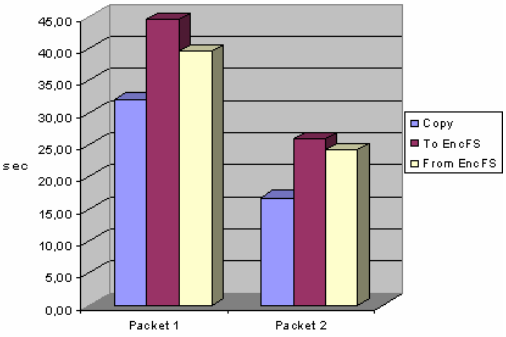
	Packet 1	*Packet 2*
1. Copy	37,78s	42,06s
2. To EFS	41,62s	47,50s
3. From EFS	60,65s	105,89s



Sl. 5. Grafički prikaz perfromansi za Windows

TABELA 2: REZULTATI ZA LINUX PLATFORMU

	Packet 1	*Packet 2*
1. Copy	32,06s	16,74s
2. To EncFS	44,45s	25,85s
3. From EncFS	39,49s	24,15s



Sl. 6. Grafički prikaz performansi za Linux

Tabela 1 i tabela 2 daju pregled ostvarenih vremena za pojedine testove i iskazane su u sekundama. Brojevi ispred vrste testa pokazuju na odgovarajući deo testa, kako je navedeno kod opisa testa. Sl. 5. i sl. 6. daju grafički pregled istih podataka radi lakšeg vizuelnog uočavanja. Podaci se odnose na Windows i Linux platforme, redom, i na paket 1 i paket 2, redom.

TABELA 3: POKAZATELJI POVEĆANJA ZA WINDOWS

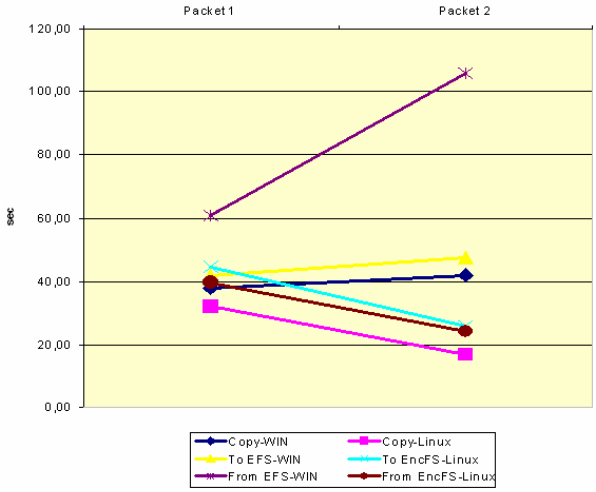
Packet1: Copy/To EFS	10,15%
Packet2: Copy/To EFS	12,94%
Packet1: Copy/From EFS	60,53%
Packet2: Copy/From EFS	151,77%

TABELA 4: POKAZATELJI POVEĆANJA ZA LINUX

Packet1: Copy/To EFS	38,65%
Packet2: Copy/To EFS	54,46%
Packet1: Copy/From EFS	23,16%
Packet2: Copy/From EFS	44,28%

Tabele 3 i 4 pokazuju koliko je došlo do povećanja dužine trajanja kopiranja u i iz kriptovanog direktorijuma u odnosu na test običnog kopiranja. Na primer, prvi red tabele 3 kaže da je potrebno 10,15% više vremena u odnosu na obično kopiranje da bi se paket 1 prekopirao u kriptovani direktorijum, sve na Windows platformi.

Na sl. 7. je dat uporedni grafički prikaz rezultata svih testova na obe platforme.



Sl. 7. Uporedni prikaz performansi na obe platforme

V. ZAKLJUČAK

Iz datih tabela i grafikona se vidi da je EFS skoro uvek sporiji od EncFS-a (čak je NTFS sporiji od ext3 fajl sistema). Delimični razlog tome može biti da EFS koristi ključ dužine 256 bita za AES, dok EncFS podrazumevano koristi 192 bita.

Takođe se može zaključiti da korišćenje enkripcionog datotečnog sloja unosi dodatno usporenje pri radu.

LITERATURA

[1] Microsoft TechNet, www.microsoft.com, ključna reč za pretragu "efs", septembar 2008.

[2] D. Pilipović, D. Stjepanović: „Karakteristike sigurnosti Encrypting File System-a", Infoteh, Jahorina, 2008.

[3] Wikipedia-the free encyclopedia, www.wikipedia.org, ključne reči za pretragu "nfts" i "encfs", septembar 2008.

[4] B. Đorđević, V. Timčenko, D. Ilić: "Komparacija sistema datoteka na Linux kernelu 2.6", Telfor, Beograd, 2007.

[5] B. Đorđević, D. Pleskonjić, N. Maček: "Operativni sistemi", Mikro knjiga, Beograd, 2005.

[6] V. Gough: http://www.arg0.net/encfs, septembar 2008.

ABSTRACT

In today world of everything connecting everything, data easy become information, thus implementation of data security is important. Encryption is obligatory tool of security. Because of that, in this paper will be presented performance of encrypting file systems on tipical PC.

ENCRYPTING PERFORMANCE OF FILE SYSTEMS.

Dragoljub Pilipović, Dejan Stjepanović.