OS2019 - Projekat II faza

OS encryption

Cilj druge faze projekta je dopuniti mehanizam za enkripciju i dekripciju za Linux 0.0.1 sa nekim bitnim funkcionalnostima. Domaći se piše u C i assembly unutar Linux 0.0.1 kernela. Kompletan projekat treba da podrži sledeće funkcionalnosti:

- Enkripcija direktorijuma
    - Podrazumeva enkripciju svih datoteka unutar direktorijuma, kao i datoteka u poddirektorijumima.
- Keširanje ključa na određeno vreme, lokalno i globalno. Keš se ne nasleđuje kod child procesa.
- Pamćenje ključa za enkriptovane datoteke, kako bi se izbeglo kvarenje datoteka upotrebom pogrešnog ključa.
- Alat za postavljanje ključa koji ne ispisuje ključ na ekranu.

Modifikacije

U okviru prve faze projekta, razvijen je sistem za automatsko enkriptovanje i dekriptovanje datoteka koje su deo Linux 0.0.1 fajl sistema. Za drugu fazu je neophodno uvesti nekoliko bitnih modifikacija u ovaj sistem.

1 Enkripcija / dekripcija direktorijuma

Ako korisnik izvrši sistemski poziv za enkriptovanje (pomoću alata `encr`) nad direktorijumom, dešava se sledeće:

- Enkriptuju se sve datoteke unutar direktorijuma, kao i sam direktorijum.
- Za svaki poddirektorijum unutar zadatog direktorijuma se ponavlja ista operacija.

Ova logika treba da bude ugrađena u sam sistemski poziv, ne u alat `encr`. Sistemski poziv i dalje ne funkcioniše ako ključ nije setovan.

Alat i sistemski poziv `decr` treba da radi na isti ovaj način kada je pozvan nad direktorijumom.

2 Keširanje ključa na ograničeno vreme

Izmeniti sistemski poziv `keyset` tako da može da postavi globalni ili lokalni ključ. Svaki proces treba da ima svoj lokalni ključ koji može da postavi pomoću ovako modifikovanog `keyset` poziva. `keyset` tool i dalje postavlja globalni ključ.

Za svaki proces sistem pamti kad je zadnji put pozvao `keyset` i ako prođe ordeđeno vreme (za testiranje postaviti 45 sec) sistem automatski briše ključ za taj proces (kao da je pozvan **sistemski poziv** `keyclear` koji radi lokalno).

Globalni ključ treba da se prazni 2 min posle postavljanja.

`keyclear` poziv modifikovati da čisti ili globalni ili lokalni ključ, dok `keyclear` tool i dalje čisti globalni.

Fork-ovani procesi ne treba da naslede keširan ključ roditelja.

3 Pamćenje ključa za enkriptovane datoteke

U prvoj fazi projekta nismo pamtili kojim ključem je datoteka enkriptovana, tako da pokušaj dekripcije sa pogrešnim ključem dovodi do trajnog uništavanja datoteke.

Taj problem sada treba rešiti tako što se pri enkriptovanju datoteke beleži i hash vrednost ključa sa kojim je ona enkriptovana. Odabrati ili neku dobro poznatu funkciju za heširanje ili implementirati svoju. Ako se pokuša pristup datoteci (`decr` / `read` / `write`) sa pogrešnim ključem, umesto dekriptovanja treba vratiti kod o grešci -EINVAL.

Ako je urađena stavka 1, pri dekriptovanju će operacija biti uspešna samo nad datotekama koje su enkriptovane sa trenutno postavljenim ključem.

4 Modifikacija keyset alata

Pri postavljanju ključa pomoću `keyset` alata, ključ se više ne zadaje kao argument na komandnoj linji. Alat se startuje bez argumenata, i od korisnika se očekuje da unese ključ po startovanju alata. Karakteri koje korisnik unosi treba da se ne prikazuju na ekranu za vreme unosa.

Predaja i rokovi

Zadatak se predaje putem mail-a na bmilojkovic@raf.rs ili mveniger@raf.rs. Neophodno je arhivirati i šifrovati urađen zadatak kako bi sigurno mogao da se pošalje preko Google mail. Uputstvo za slanje:

- Kompletan linux-0.01/ direktoijum sa domaćim zadatkom smestiti u direktorijum koji se zove "os_proj2_ime_prezime_ind".
    - Npr. "os_proj2_student_studentic_rn0101".
- Arhivirati ovaj direktorijum (.zip) i nazvati arhivu isto kao direktorijum sa .zip ekstenzijom (u Ubuntu pronaći direktorijum, desni klik, opcija compress)
- U terminalu se postaviti u direktorijum gde se nalazi arhiva i šifrovati je pomoću komande:
- gpg -c <ime arhive>
    - gpg -c os_proj2_student_studentic_rn0101.zip
    - Kao šifru uneti "osos"
- Trebalo bi da se pojavi datoteka koja se zove kao arhiva, sa dodatnom ekstenzijom .gpg.
    - os_proj2_student_studentic_0101.zip.gpg
- Taj fajl poslati kao attachment uz mail.

U tekstu mail-a obavezno navesti:

- Ime i prezime
- Broj indeksa
- Grupa, po zvaničnom spisku

Subject mail-a mora da bude u obliku: "[OS] Proj2 ime_prezime_ind".
Npr. "[OS] Proj2 student_studentic_rn0101"

Naziv attachmenta mora da bude u obliku: "os_proj2_ime_prezime_ind.zip.gpg"
Npr. "os_proj2_student_studentic_rn0101.zip.gpg"

Rok za predaju je:

- Četvrtak, 13. jun 23:59:59 za sve studente.

Rok je definisan po grupi kojoj student zvanično pripada. Za studente sa starijih godina se primenjuje najkasniji rok.

Neće se pregledati zadaci (tj. biće dodeljeno 0 poena) ako se desi bilo koje od:

- Sadržaj mail-a nije po navedenom obliku.
- Subject mail-a nije po navedenom obliku.
- Naziv attachmenta nije po navedenom obliku.
- Arhiva nije dobro šifrovana.
- Predaja se desi nakon navedenog roka.

Odbrana domaćih zadataka je obavezna. Odbrane će se vršiti po grupama u subotu, 15. juna. Grupe će biti formirane i objavljene u petak 14. juna. Ako ste iz bilo kog razloga sprečeni da prisustvujete odbrani, obavezno to najavite što pre, kako bismo mogli da zakažemo vanredni termin za odbranu. Sve odbrane moraju da se završe najkasnije 15. juna. Ako ste svesni da tada niste slobodni, obavezno to najavite unapred.

Svrha odbrane je da se pokaže autentičnost zadatka. Ovo podrazumeva odgovaranje na pitanja u vezi načina izrade zadatka, ili izvršavanje neke izmene nad zadatkom na licu mesta. U slučaju da odbrana nije uspešna, dodeljuje se -10 poena na drugoj fazi projekta.

Bodovanje

Zadatak se boduje na sledeći način:

- Enkripcija / dekripcija direktorijuma - 4 poena
- Keširanje ključa - 7 poena
- Pamćenje ključa za enkriptovane datoteke - 7 poena
- Keyset alat bez ispisa na konzoli - 2 poena

Prva faza projekta urađena nakon roka za izradu prve faze se vrednuje sa 50% poena.