OS2019 - Projekat I faza

OS encryption

Cilj prve faze projekta je obezbediti mehanizam za enkripciju i dekripciju za Linux 0.0.1 pomoću transpozicione šifre. Domaći se piše u C i assembly unutar Linux 0.0.1 kernela. Enkriptovani fajlovi treba da ostanu enkriptovani i nakon gašenja i ponovnog paljenja sistema. Kompletan domaći zadatak treba da podrži sledeće funkcionalnosti:

- Korisnik može da enkriptuje / dekriptuje datoteke.
- Čitanje i pisanje pomoću standardnih sistemskih poziva treba da funkcioniše nad enkriptovanim datotekama, kao i nad normalnim datotekama.
- Korisnik može da podešava ključ pomoću kojeg se vrši enkripcija / dekripcija.
- Korisnik može da generiše nasumični ključ.

Snimak sa primerom korišćenja svih funkcionalnosti je dat na materijalima.

Kriptografski algoritam

Za potrebe enkriptovanja / dekriptovanja koristiti transpozicioni algoritam zasnovan na zameni kolona matrice, koji je opisan ovde.

Datoteka treba da se enkriptuje u blokovima od po 1024 bajta (čitav `buffer_head` bafer koji se inače koristi za čitanje i pisanje datoteka). Kao ključ se koristi niz printabilnih ASCII karaktera čija ASCII vrednost se koristi za transpoziciju. Dužina ključa će uvek biti neki stepen dvojke i manja od 1024, tako da matrica sa 1024 karaktera sigurno može da se formira sa tim brojem kolona. Ključ će uvek biti bez ponavljanja.

Spisak enkriptovanih fajlova treba zapisati na disku. Ovo može da bude u posebnoj datoteci kojoj će inače biti onemogućen pristup, ili na bloku koji je posebno namenjen za ovo i koji ne može da bude prepisan običnom datotekom. Ovu datoteku / blok treba da nikako nije moguće obrisati, prepisati, izmeniti, i sl. osim normalnim radom sistema za enkripciju / dekripciju.

Nakon što korisnik prvi put podesi ključ za enkripciju, postaje moguće čitati i pisati enkriptovane datoteke. One mogu već da budu na disku, a mogu i da se obične datoteke enkriptuju pomoću posebne komande. Funkcije `read` i `write` moraju da rade normalno i sa enkriptovanim i sa ne-enkriptovanim datotekama.

Alati

Neophodno je implementirati sledeće alate, koji će da prave odgovarajuće sistemske pozive:

`keyset <kljuc>`

Postavlja prosleđeni parametar kao trenutno aktivan globalan ključ. Dužina ključa mora da bude stepen dvojke i manji od 1024. Ako nije, prijaviti grešku. Pri prvom pozivu ovog alata se čita spisak enkriptovanih fajlova sa diska, i smešta se u memoriju. Nakon toga, svaki poziv `read` ili `write` nad enkriptovanom datotekom treba da uspešno čita, odnosno piše, tj. treba primenjivati algoritam za enkripciju / dekripciju pri izvršavanju tih poziva.

`encr <file>`

Enkriptuje zadati fajl pomoću zadatog ključa, u slučaju da nije već enkriptovan. Ako je fajl već enkriptovan, prijaviti grešku. Ovaj alat takođe treba u sistemu da zabeleži da je ovaj fajl enkriptovan. Ako ključ nije prethodno postavljen pomoću alata **`keyset`**, prijaviti grešku.

`decr <file>`

Dekriptuje zadati fajl pomoću zadatog ključa, u slučaju da je fajl prethodno enkriptovan. Ako fajl nije prethodno enkriptovan, prijaviti grešku. Ovaj alat takođe treba u sistemu da zabeleži da ovaj fajl više nije enkriptovan. Ako ključ nije prethodno postavljen pomoću alata **`keyset`**, prijaviti grešku.

`keyclear`

Resetuje ključ na `NULL`, i onemogućava dalje enkriptovanje i dekriptovanje sve dok se ne pozove **`keyset`** ponovo. Funkcije `read` i `write` treba da ponovo rade kao da nisu svesne enkripcije.

`keygen level`

Generiše nasumični ključ sačinjen od printabilnih ASCII karaktera i ispisuje ga na ekranu. Parametar **`level`** može da bude jedno od:

- 1 - generiše se ključ dužine 4;
- 2 - generiše se ključ dužine 8;
- 3 - generiše se ključ dužine 16.

Ako level nije dato, ili nije jedna od ove tri vrednosti, prijaviti grešku.

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_proj1_ime_prezime_ind".
    - Npr. "os_proj1_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_proj1_student_studentic_rn0101.zip
    - Kao šifru uneti "osos"
- Trebalo bi da se pojavi datoteka koja se zove kao arhiva, sa dodatnom ekstenzijom .gpg.
    - os_proj1_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] Proj1 ime_prezime_ind".
Npr. "[OS] Proj1 student_studentic_rn0101"

Naziv attachmenta mora da bude u obliku: "os_proj1_ime_prezime_ind.zip.gpg"
Npr. "os_proj1_student_studentic_rn0101.zip.gpg"

Rok za predaju je:

- Ponedeljak, 27. maj 23:59:59 za grupe koje slušaju OS ponedeljkom
- Četvrtak, 30. maj 23:59:59 za grupe koje slušaju OS četvrtkom
- Petak, 31. maj 23:59:59 za grupe koje slušaju OS petkom

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. Grupe će biti formirane i objavljene u subotu 1. 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.

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 prvoj fazi projekta.

Bodovanje

Zadatak se boduje na sledeći način:

- Enkripcija / dekripcija (`keyset`, `keyclear`, `encr`, `decr`) - 7 poena
- `read` i `write` funkcionišu nad enkriptovanim datotekama - 5 poena
- Čuvanje spiska enkriptovanih datoteka na disku - 5 poena
- Generisanje ključa - 3 poena