Elektrotehnički fakultet Banja Luka
Katedra za računarsku tehniku i informatiku
Kriptografija i računarska zaštita
Projektni zadatak

Zadatak

Realizovati jednostavan sistem koji predstavlja dijeljeni enkriptovani fajl sistem (EFS) za više korisnika. Korisnik se prijavljuje na sistem pomoću korisničkog imena i lozinke i validnog digitalnog sertifikata. Nakon prijave na sistem, korisnik vidi kompletno stablo direktorijuma čiji je korijen *home* direktorijum koji je predstavljen korisničkim imenom prijavljenog korisnika. Kompletan sadržaj fajl sistema treba da bude zaštićen, pri čemu svaki korisnik može da vidi samo svoje direktorijume i datoteke. Potrebno je podržati minimalno tekstualne, PDF datoteke, kao i slike. Sistem treba da onemogući korištenje datoteka čiji je integritet narušen.

Prijavljeni korisnik može da dodaje nove datoteke na EFS i da preuzima postojeće datoteke sa EFS-a na *host* fajl sistem. Prilikom dodavanja, navodi se putanja do datoteke na *host* fajl sistemu, kao i putanja do direktorijuma u kojem će biti smještena nova datoteka na EFS-u. Prilikom preuzimanja, datoteku je potrebno dekriptovati. Takođe, korisnik može da kreira nove i briše postojeće direktorijume (uključujući kompletan sadržaj).

Sistem nudi i jednostavan način za dijeljenje datoteka, pomoću jedinstvenog dijeljenog direktorijuma. Korisnik koji želi podijeliti datoteku sa drugim korisnikom, treba da ostavi datoteku u dijeljeni direktorijum, tako da je samo korisnik kojem je namijenjena može preuzeti. Voditi računa da sadržaj dijeljenog direktorijuma mogu da vide svi korisnici sistema.

Obratiti pažnju na brzinu aplikacije, u smislu ispravnog korištenja simetričnih i asimetričnih algoritama (iskoristiti onaj algoritam koji će u datom slučaju dati najbolje performanse, a da sigurnost sistema nije narušena). Potrebno je podržati barem tri različita algoritma za enkripciju i tri algoritma za heširanje.

Na proizvoljan način realizovati čuvanje korisničkih naloga, kao i veze između korisničkog naloga i sertifikata. Procedura kreiranja korisničkog naloga, kao i odgovarajućeg *home* direktorijuma, treba biti realizovana kroz aplikaciju.

Aplikacija podrazumijeva postojanje infrastrukture javnog ključa. Svi sertifikati treba da budu izdati od strane CA tijela koje je uspostavljeno prije početka rada aplikacije. Sertifikati se generišu nekim eksternim sistemom. Podrazumijevati da će se na proizvoljnoj lokaciji na fajl sistemu nalaziti CA sertifikat, CRL lista, sertifikati svih korisnika, kao i privatni ključ trenutno prijavljenog korisnika. Validaciju sertifikata je potrebno vršiti u trenutku njegove upotrebe.

Sve detalje zadatka koji nisu precizno specifikovani realizovati na proizvoljan način. Dozvoljena je upotreba proizvoljnog programskog jezika i odgovarajuće biblioteke za realizaciju kriptografskih funkcija (npr. *Bouncy Castle*). Način realizacije korisničkog interfejsa neće biti ocjenjivan.

Projektni zadatak važi od prvog termina januarsko-februarskog ispitnog roka 2025. godine i vrijedi do objavljivanja sljedećeg projektnog zadatka.