Elektrotehnički fakultet Banja Luka
Katedra za računarsku tehniku i informatiku
Kriptografija i računarska zaštita (2256) / Kriptografija i kompjuterska zaštita (A810)
Projektni zadatak

Zadatak

Napisati *chat* aplikaciju koja omogućava zaštićenu komunikaciju između korisnika bez korištenja ugrađenih klasa koje omogućavaju datu funkcionalnost. Aplikacija treba da omogući razmjenu poruka između dva korisnika putem ostavljanja datoteka na određenim lokacijama na fajl sistemu.

Po prijavi na sistem, aplikacija prikazuje informacije o trenutno aktivnim korisnicima, pri čemu prijavljeni korisnik bira korisnika sa kojim će započeti sesiju. Oba korisnika treba da daju saglasnost za učešće u sesiji, prije početka dopisivanja. Proces započinjanja, trajanja i završetka sesije treba realizovati na aplikativnom sloju OSI modela, uz sopstvenu implementaciju aplikativnog komunikacionog protokola. Sva komunikacija između učesnika sesije treba da bude zaštićena, uz adekvatno korištenje kriptografskih tehnika i algoritama.

Prva i posljednja poruka u okviru sesije, treba da budu dodatno sakrivene uz pomoć tehnike steganografije. Prilikom slanja ovih poruka, potrebno je navesti putanju do slike u kojoj će poruka biti sakrivena, nakon enkripcije. Steganografski algoritam definisati na proizvoljan način, ali tako da kvalitet slike bude minimalno narušen. Voditi računa o dužini poruke i kapacitetu koji slika ima za ovu namjenu.

Chat funkcionalnost treba realizovati uz pomoć fajl sistema koji, u ovom slučaju, simulira distribuiranu klijent-server platformu za komunikaciju udaljenih korisnika. Podrazumijevano, svakom korisniku treba pridružiti odgovarajući direktorijum, koji će predstavljati njegov *inbox*. Aplikacija treba da, za prijavljenog korisnika, prati i detektuje promjene u njegovom direktorijumu, tj. detektuje pristizanje novih poruka. Nakon što korisnik unutar aplikacije pročita poruku, ona se briše sa fajl sistema.

Prijava na sistem podrazumijeva unos korisničkog imena i lozinke. Na proizvoljan način realizovati čuvanje korisničkih naloga, kao i veze između korisničkog naloga i sertifikata. Procedura kreiranja korisničkih naloga ne mora 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.

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 algoritma za enkripciju i tri algoritma za heširanje.

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.

Studenti su dužni da kontaktiraju predmetnog asistenta najkasnije sedam dana prije ispitnog roka za koji su prijavili ispit kako bi se odredio termin odbrane projektnog zadatka. Potrebno je predati kompletan izvorni kod aplikacije (NetBeans, Eclipse, Visual Studio ili neki drugi projekat).

Projektni zadatak važi od prvog termina januarsko-februarskog ispitnog roka 2020. godine za predmete Kriptografija i računarska zaštita (III godina) i Kriptografija i kompjuterska zaštita (IV godina). Početkom važenja ovog projektnog zadatka prestaju važiti svi raniji projektni zadaci. Studenti koji do januarsko-februarskog ispitnog roka ne polože kompletan ispit moraju raditi novi projektni zadatak, bez obzira na datum odbrane prethodnog projektnog zadatka. Odbranjen projektni zadatak važi do objavljivanja teksta sljedećeg projektnog zadatka.