Elektrotehnički fakultet Banja Luka
Katedra za računarsku tehniku i informatiku
Kriptografija i računarska zaštita
Projektni zadatak, februar 2018. godine

Zadatak

Napisati aplikaciju koja korisnicima omogućava razmjenu poruka upotrebom tehnike steganografije. Aplikacija omogućava prijavljenom korisniku da ostavi poruku proizvoljne dužine bilo kojem drugom korisniku na sistemu.

Korisnici se na sistem prijavljuju korištenjem korisničkog imena i lozinke. Aplikaciji su (u posebno definisanom direktorijumu) dostupni digitalni sertifikati za sve korisnike koji imaju nalog na sistemu. Nakon prijave, aplikacija prikazuje broj nepročitanih poruka za datog korisnika. Aplikacija čuva samo digitalne sertifikate korisnika, pa je potrebno od korisnika tražiti unos bilo kakvih dodatnih informacija potrebnih za dekripciju poruke. Nakon dekripcije, poruka, vrijeme slanja i naziv pošiljaoca se prikazuje na ekranu, a slika u kojoj se poruka nalazila se briše sa sistema. Do trenutka dekripcije, aplikaciji nije poznato koji korisnik je poslao poruku (sve informacije vezano za pošiljaoca i sadržaj poruke se čuvaju u slici).

Postupak slanja nove poruke se odvija na sljedeći način: korisnik bira korisnika kojem želi poslati poruku, unosi sadržaj poruke i putanju do slike u kojoj će poruka nakon enkripcije biti uskladištena. Slanje poruke je dozvoljeno samo ako sertifikat primaoca nije istekao u trenutku slanja. Aplikacija vodi evidenciju samo o broju primljenih poruka za nekog korisnika (tj. putanji do datoteka), dok su sve ostale informacije dostupne samo korisniku koji je primalac poruke (vrijeme slanja, pošiljalac i sadržaj). Obavezno je potrebno onemogućiti korisniku koji ima pristup fajl sistemu da obriše neku od slika i tako uništi neku poruku (tačnije, nije moguće spriječiti brisanje slika, ali aplikacija mora registrovati situaciju u kojoj je neka slika obrisana izvan aplikacije).

Steganografski algoritam definisati na proizvoljan način, ali tako da kvalitet slike bude minimalno narušen. To uključuje određivanje minimalne veličine slike, kao i definisanje postupka u slučaju da slika nije dovoljne veličine za skladištenje date poruke.

Uspostavljanje infrastrukture javnog ključa je dozvoljeno izvršiti proizvoljnim eksternim alatom, pri čemu svi sertifikati moraju biti izdati od zajedničkog sertifikacionog tijela. Novi korisnički nalozi će uvijek biti kreirani manuelno, izvan aplikacije, ali lozinke moraju biti sačuvane na siguran način (tj. ne smije biti moguće saznati lozinku nekog drugog korisnika). Smatrati da testiranje sigurnosti aplikacije neće uključivati izmjenu sadržaja direktorijuma sa digitalnim sertifikatima (tj. podrazumijevati da će sertifikati uvijek biti dostupni ako postoji nalog i da dati sertifikat sigurno pripada datom korisniku – način kodovanja informacija o nalogu u sertifikatu izabrati proizvoljno).

Tehničke detalje koji nisu eksplicitno definisani zadatkom je potrebno realizovati na proizvoljan način, ali tako da se ispune svi sigurnosni zahtjevi koji su eksplicitno navedeni u tekstu. Način realizacije korisničkog intefejsa neće biti ocjenjivan (aplikacija može biti realizovana kao konzolna ili može imati grafički interfejs).

Za realizaciju zadatka je dozvoljena upotreba bilo kojeg programskog jezika i odgovarajuće biblioteke za realizaciju kriptografskih funkcija (npr. Bouncy Castle).

Odbrana projektnog zadatka se organizuje prije svakog ispitnog roka. Potrebno je predati kompletan izvorni kod aplikacije (NetBeans, Eclipse, Visual Studio ili neki drugi projekat), kako bi se aplikacija mogla testirati na laboratorijskoj opremi.

Studenti koji brane projektni zadatak su dužni da se nekoliko dana prije ispitnog roka za koji su prijavili ispit jave predmetnom asistentu kako bi se odredio termin za odbranu projektnog zadatka.

Projektni zadatak važi od prvog termina februarskog ispitnog roka 2018. 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 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.