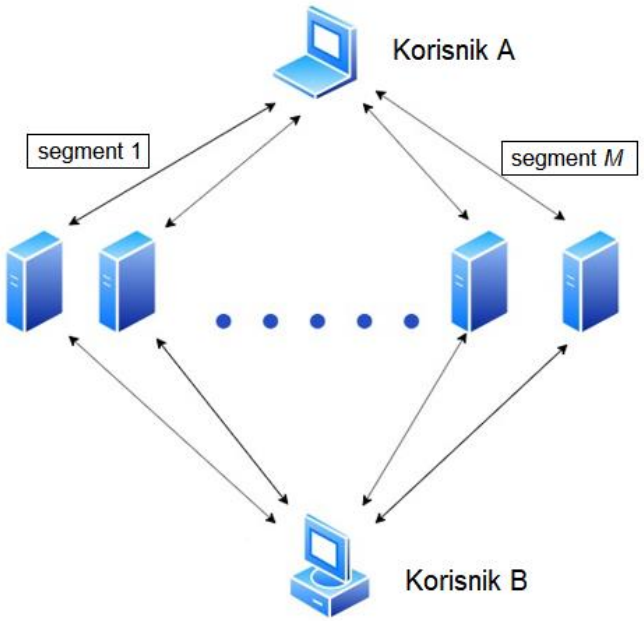
Elektrotehnički fakultet Banja Luka
Katedra za računarstvo i informatiku
Sigurnost na internetu
Projektni zadatak

Zadatak

Implementirati *web* bazirani sistem za anonimnu komunikaciju na bazi standardnih sistema za razmjenu poruka. Sistem treba da funkcioniše na principu mješovitih mreža koji je sličan principu TOR[1] mreže.

Svaka poruka se prije slanja dijeli na *M* segmenata (*M*≥3, slučajno generisana vrijednost), pri čemu se svaki od tih segmenata šalje ka jednom od *N* servera (3≤*N*≤4). Ako je *N*=*M*, onda svaki server prihvata samo jedan segment poruke u toku slanja te poruke od pošiljaoca ka primaocu. Svaki server primljeni segment poruke prosljeđuje do primaoca koji, kada prihvati svih *M* segmenata, vrši rekonstrukciju poruke (slika 1).



Slika 1 – Arhitektura sistema

Sistem treba biti zasnovan na klijent-server arhitekturi, pri čemu se, umjesto jednog, koristi *N* servera. Za simulaciju servera, dozvoljeno je korištenje više virtuelnih mašina, ili više instanci odgovarajućeg servera na istoj mašini, pri čemu je potrebno da barem jedan korisnik bude prijavljen na drugoj (virtuelnoj) mašini.

Za implementaciju komunikacionog kanala između klijenta i servera, dozvoljeno je iskoristiti neki od postojećih protokola za razmjenu poruka, kao što je XMPP, MQ, JMS i sl, odnosno neku od *open-source* implementacija ovih protokola (XMPP Openfire, RabbitMQ, ActiveMQ i sl.).

Protokol komunikacije je potrebno definisati na proizvoljan način (način segmentacije poruke i rekonstrukcije segmenata, vrijeme i redoslijed slanja pojedinih

[1] https://www.torproject.org/

segmenata, označavanje rednog broja segmenta, upotreba kriptografskih tehnika i način razmjene ključeva i ostalih informacija itd.).

Korisnik se prijavljuje na sistem pomoću svojih kredencijala, nakon čega mu se prikazuje lista prijavljenih korisnika. Nakon toga, korisnik bira korisnika sa kojim želi da komunicira. Detalje korisničkog interfejsa realizovati na proizvoljan način.

U cilju zaštite podataka i povećanja nivoa anonimnosti korisnika, potrebno je iskoristiti odgovarajuće kriptografske tehnike i algoritme. Da bi se sigurnost sistema dodatno povećala, potrebno je jedan dio svake poruke slati pomoću tehnike steganografije (koristiti slike).

Sve detalje zadatka koji nisu precizno specifikovani realizovati na proizvoljan način. Dozvoljena je upotreba proizvoljnog programskog jezika, kao i proizvoljnih tehnologija neophodnih za realizaciju tehničkih detalja.

Studenti koji uspješno odbrane projektni zadatak stiču pravo izlaska na usmeni dio ispita. Prije odbrane, potrebno je postaviti kompletan izvorni kod projektnog zadatka na *moodle*. Projektni zadatak važi od prvog termina januarsko-februarskog ispitnog roka 2023. godine i vrijedi do objavljivanja sljedećeg projektnog zadatka.