Secure Internet Relay Chat

Projekt Secure Internet Relay Chat si dáva za cieľ vytvoriť platformu, ktorá umožní jeho používateľom bezpečnú vzájomnú komunikáciu a zdieľanie multimediálneho obsahu. Skladá sa z dvoch časti a to konkrétne zo serveru a z klientskej aplikácie.

Server umožní klientom prihlásenie pod zvoleným pseudonymom. Nebude sa jednať o klasickú registráciu pomocou mena a hesla, pri ktorej si server tieto údaje ukladá, čo by umožnilo čiastočné sledovanie aktivity používateľov. V našom riešení sa užívateľ identifikuje iba unikátnym pseudonymom, pričom pre každé nové sedenie si môže tento identifikátor zvoliť nový čím sa snažíme dosiahnuť ďalšie zvýšenie anonymity. Okrem „registrácie“ bude server poskytovať zoznam aktuálne prihlásených užívateľov a zabezpečovať inicializáciu spojenia dvoch klientov.

Klientska aplikácia bude slúžiť k prihláseniu na server a samotnú komunikáciu medzi klientami. Po nadviazaní spojenia bude komunikácia prebiehať vo forme peer-to-peer, pričom prenášané dáta budú šifrované symetrickou šifrou AES_{256}.

Zabezpečenie

Kompromitácia servera

V prípade kompromitácie servera musíme riešiť zabezpečenie anonymity klientov. To sa snažíme dosiahnuť mazaním logov zaznamenávajúcich sieťovú komunikáciu. Útočník je teda schopný získať informácie iba o aktuálne pripojených klientoch (napríklad z operačnej pamäte).

Komunikácia so serverom

Pri komunikácii so serverom je nutne dosiahnuť anonymity klienta a zabezpečiť bezpečnú komunikáciu. Anonymita klienta je dosiahnutá pomocou siete TOR. Klient sa k serveru pripája pomocou tejto siete, čo znemožňuje jednoduché zistenie že sa pripojil pravé k nášmu serveru.

Všetka komunikácia klienta so serverom prebieha pomocou protokolu TLS. Verejný kľúč servera (S_{PB}) je verejne dostupný a pre každého klienta rovnaký. Nakoľko sa tento kľúč nemení a jeho prelomenie nebolo jednoduché je nutne zvoliť dostatočné veľký kľúč. Po pripojení klientska aplikácia vygeneruje svoj verejný (K_{PB}) a privátny (K_{PR}) kľúč asymetrickej šifry RSA. Svoj verejný kľúč zašifruje verejným kľúčom servera a odošle ho serveru. Všetka nasledujúca komunikácia medzi klientskou aplikáciou a serverom je šifrovaná pomocou týchto kľúčov. Týmto sa snažíme zabezpečiť komunikáciu proti útočníkom ktorý sú schopný sledovať ale aj modifikovať sieťovú komunikáciu medzi klientom a serverom.

Kompromitácia klient

Na zabezpečenie klienta naša aplikácia nemá veľký dosah. Pokiaľ útočník kompromituje klientsky počítač je schopný zistiť informácie o aktuálnych pripojeniach ako aj rôzne informácie zo systémových logov.

Komunikácia medzi klientami

Po inicializácii spojenia medzi klientami, server každému z nich zdali verejný kľúč druhého účastníka. Klient, ktorý inicializoval spojenie vytvorí TLS spojenie s požadovaným klientom. Následne vygeneruje kľúč pre symetrickú šifru, zašifruje ho verejným kľúčom partnera a odošle mu ho. Všetka ďalšia komunikácia medzi klientami už prebieha šifrované pomocou tohto kľúča. Rovnako ako pri serveri sa snažíme zabezpečiť komunikáciu voči sledovaniu ale aj proti útoku MITM.

Popis funkcionality

Server

- **REGISTRATION_CONFIRM –** po prijatí žiadosti na prihlásenie klienta, server skontroluje či nie je požadovaný pseudonym už používaný. V prípade že nie, klienta prihlási a odošle mu potvrdenie o úspešnom prihlásení. Spolu so zvoleným pseudonymom je uložený aj verejný kľuč a IP adresa klienta s portom, na ktorom naslúcha.

- **REGISTRATION_REJECT –** oznámenie klientovi že sa pod zvoleným pseudonymom nepodarilo prihlásiť.

- **LEAVE_CONFIRM –** odhlásenie klienta.

- **SEND_LIST –** po prijatí správy *GET_LIST* od klientskej aplikácie, server odošle zoznam aktuálne prihlásených pseudonymov.

- **CONNECT_REQUEST –** server po prijatí požiadavky o spojenie s druhým používateľom overí existenciu zadaného pseudonymu. V prípade úspechu pošle danému klientovi požiadavku o spojenie.

- **REQUEST_FAIL –** oznámenie používateľovi, že sa pokúša spojiť s neexistujúcim pseudonymom alebo oznámenie, že protistrana spojenie odmietla.

- **SEND_USER_INFO –** po potvrdení požiadavku o spojení s klientom, sú obom účastníkom zaslané informácie o ich partnerovi (verejný kľúč a IP adresa s portom).

Klientska aplikácia

Komunikácia so serverom:

- **REGISTRATION –** požiadavka na server o prihlásenie pod zvoleným pseudonymom.

- **LEAVE –** požiadavka o odhlásenie pseudonymu.

- **GET_LIST –** požiadavka o zoznam aktuálne prihlásených pseudonymov.

- **SEND_REQUEST –** požiadavka o nadviazanie spojenia s druhým klientom. Táto správa je zaslaná na server, ktorý následne overí existenciu zadaného pseudonymu. Po úspešnom overení prepošle túto požiadavku zodpovedajúcemu klientovi.

- **REQUEST_CONFIRM –** prijatie požiadavku o spojenie s druhým klientom.

- **REQUEST_REJECT –** odmietnutie požiadavku spojenie s druhým klientom.

Komunikácia s druhým klientom:

- **CREATE_CHANEL –** v prípade súhlasu partnera s požiadavkou o komunikáciu sa s týmto klientom vytvorí priamy, zabezpečený kanál (viz. Zabezpečenie).

- **DELETE_CHANEL –** pri ukončení spojenia s klientom sa uzavrie socket a uvoľní pamäť s už nepotrebnými informáciami.

- **SEND_MESSAGE –** odoslanie správy partnerovi, spolu s telom správy je poslaný aj čas odoslania.

- **SEND_FILE –** požiadavka na odoslanie multimediálneho obsahu partnerovi.

- **FILE_ CONFIRM –** prijatie multimediálneho obsahu odoslaného partnerom.

- **FILE_ REJECT –** odmietnutie multimediálneho obsahu odoslaného partnerom.