Politechnika Poznańska

Wydział informatyki i telekomunikacji

Dokumentacja projektu

Dokumentacja projektu z zajęć Telefonia IP

Autorzy:

Adrian Golczak 136239
adrian.e.golczak@student.put.poznan.pl

Marcin Kubiak 136267
marcin.w.kubiak@student.put.poznan.pl

Wersja: v1.0.0

19.03.2020 r.

Spis treści

1 Charakterystyka ogólna projektu

Przedmiotem projektu pt. 'Opracowanie bezpiecznego systemu komunikacji głosowej w sieci IP (VoIP) wraz z jego implementacją' jest opracowanie aplikacji mobilnej na urządzenia z systemem Android wyposażonej w algorytmy RSA oraz AES-256 umożliwiające bezpieczną rozmowę pomiędzy dwoma użytkownikami aplikacji. Aplikacja będzie zaprojektowana tak, że osoba trzecia będzie w stanie podsłuchać tylko niewrażliwe dane, dzięki zastosowaniu RSA oraz AES-256. Główną koncepcją projektu jest stworzenie tzw. poczekalni, w której zalogowani użytkownicy bedą mogli się łączyć z kim tylko chcą i odbywać z nim rozmowę. W celu bezpieczeństwa, użytkownicy będą generować klucze publiczne oraz prywatne, które następnie będą używane do szyfrowania, deszyfrowania oraz przesyłaniu klucza szyfru blokowego AES, służącego do szyfrowania rozmowy. Aplikacja ma być łatwa w obsłudze oraz przejrzysta, dlatego będzie ograniczać się tylko do przyjmowania, odrzucania połączenia oraz rozmowy między dwoma użytkownikami.

2 Architektura systemu

System oparty jest o architekturę klient - serwer. Aplikacja kliencka zainstalowana została na urządzeniu mobilnym. Jej zadaniem jest udostępnienie interfejsu dla użytkownika w taki sposób aby w prosty sposób umożliwić korzystanie z usług serwera. Aplikacja zapewnia również poziom bezpieczeństwa szyfrując/deszyfrując aplikację (serwer pełni rolę pośrednika, nie uczestniczy w komunikacji, nie jest w stanie "podsłuchaćżozmowy, gdyż ta jest szyfrowana.) W architekturze definiujemy 3 byty uczestniczące w procesie komunikacji:

- *Serwer* - aplikacja napisana w języku Java z użyciem frameworka Spring Boot. Jest instalowana na urządzeniu z wystarczającymi zasobami do zarządzania komunikacją (np. laptop, przy założeniu, że ilość rządań będzie nieznaczna).
- *Klient* - aplikacja na urządzenia mobilne z systemem Android.
- *Użytkownik* - osoba posiadająca zainstalowaną aplikację wraz z wylosowanym (przez serwer) unikalnym id.
- *Osoba akceptująca połączenie* - jest to użytkownik, który otrzymał informację poprzez interfejs, że inny użytkownik chce się z nim połączyć.

Użytkownik po uruchomieniu aplikacji klienckiej zostaje poproszony o wpisanie pseudonimu (pod warunkiem, że nie został już wpisany), następnie klient wysyła rządanie do serwera o źarejestrowanie", rządanie składa się z wylosowanego uprzednio klucza publicznego, a także pseudonimu użytkownika. Serwer dodaje klienta do kolejki nadając mu unikalny identyfikator, od tej pory komunikacja oparta jest o ten identyfikator. W momencie w którym

użytkownik zechce połączyć się innym użytkownikiem klient wysyła rządanie do serwera o sparowanie dwóch użytkowników (drugim jest osoba akceptująca połączenie). Jeśli połączenie zostanie zaakceptowane serwer tworzy sesję, a następnie wysyła odpowiednie komunikaty wraz z odpowiednimi kluczami publicznymi do klientów. Aplikacje mobilne używają kluczy publicznych do wylosowania 256 bitowego klucza AES po 128 bitów każdy, gdzie pierwsze 128 bitów należy do osoby rządającej połączenia, a ostatnie 128 bitów należy do osoby akceptującej. Obie strony wymieniają się zaszyfrowanymi częściami klucza, ostatnim krokiem jest potwierdzenie otrzymania części drugiej strony. Od tego momentu komunikacja jest szyfrowana AES-256, aż do zakończenia rozmowy.

3 Wymagania

Poniżej opisane zostaną wymagania funkcjonalne i niefunkcjonalne aplikacji, z wyróżnieniem różnych stanów użytkownika.

3.1 Funkcjonalne

Użytkownik niezalogowany:

- Podanie pseudonimu
- Logowanie się do poczekalni

Użytkownik zalogowany:

- Wysyłanie próśb o połączenie
- Akceptacja prośby od drugiego użytkownika
- Generowanie klucza publicznego i prywatnego wykorzystując algorytm RSA
- Odrzucenie prośby o połączenie
- Opuszczenie poczekalni oraz trwającej rozmowy

3.2 Niefunkcjonalne

- Łączenie dwóch użytkowników
- Generowanie ID sesji
- Negocjacje klucza o rozmiarze 256 bitów na potrzeby AES-256
- Szyfrowanie rozmowy wykorzystując AES-256
- Minimalna wersja systemu Android: 10.0.0

4 Technologie, narzędzia, środowisko, biblioteki, kodeki

W procesie tworzenia systemu zostaną wykorzystane technologie i narzędzia umożliwiające komunikację pomiędzy klientami, ułatwiające pisanie dokumentacji, a także upraszczające proces pisania kodu źródłowego. Użyte zostaną między innymi:

- *TeXstudio*
- *InteliJ*
- *Java11*
- *SpringBoot*
- *AndroidStudio*
- *javax.sound*
- *jcodec*