Proiect IC

Aplicatie client-server folosind procedeul de end-to-end encryption

Mihailescu Alexandru, Grupa 343C2, 2022

Introducere

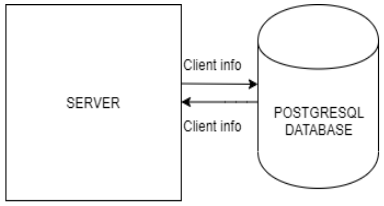
Criptarea end-to-end(E2EE) este un sistem de comunicatii in care numai utilizatorii care comunica pot citi mesajele. In principal, previne o entitate neparticipanta la conversatie care vrea sa “traga cu urechea” din a putea accesa cheile criptografice necesare pentru a decripta conversatia(provideri telecom, provideri internet, chiar si provider-ul serviciului de comunicatii).

Criptarea end-to-end intentioneaza sa previna datele din a fi citite sau modificate in secret de catre altcineva decat adevaratii expeditori si destinatari.

Pentru a intelege avantajele criptarii end-to-end, trebuie sa discutam despre celalalt mod de a cripta date(criptarea in transit). Acest tip de criptare asigura criptarea datelor numai cand acestea sunt in transit, fiind considerate cel mai vulnerabile atunci.

Spre deosebire de encryption in transit, criptarea end-to-end asigura criptarea mesajului pana cand acesta paraseste device-ul expeditorului si decriptarea sa numai cand a ajuns pe device-ul destinatarului.

Arhitectura aplicatie



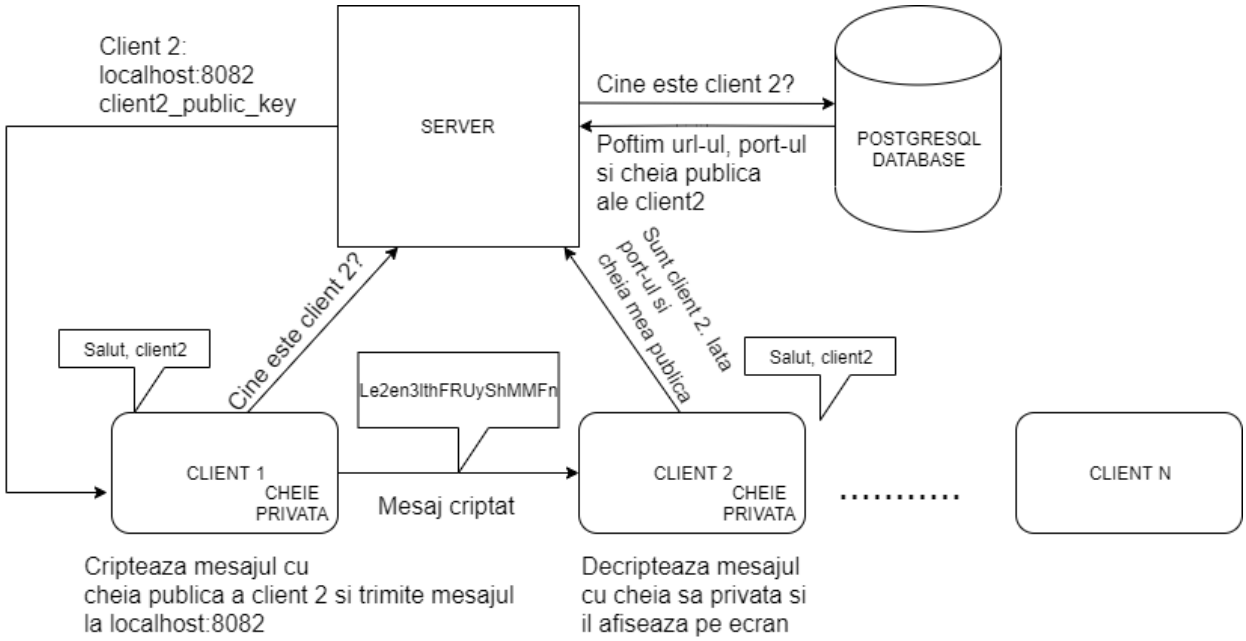
Mod de functionare al aplicatiei

Aplicatia este compusa dintr-un server central care este conectat la o baza de date SQL ce tine date despre clientii care s-au inscris in reteaua de clienti(id-uri client, chei publice, port-ul pe care ruleaza) si o serie de client care doresc sa comunice prin mesaje criptate.

Odata pornit un client, acesta isi realizeaza automat o operatie de initializare, generand o pereche cheie publica – cheie privata. Apoi, trimite date de identificare(nume, port), dar si cheia publica catre server pentru a realiza operatia de inregistrare pe server. Este de retinut faptul ca operatia de initializare(si implicit generarea celor 2 chei) se face de fiecare data la pornire(daca exista deja in baza de date a server-ului o cheie publica corespunzatoare client-ului, aceasta este suprascrisa).

Cand un client doreste sa comunice cu altul, acesta face mai intai o cerere catre server pentru a afla detaliile clientului cu care doreste sa comunice. Server-ul primeste request-ul si raspunde cu detaliile cerute(port si cheie publica). Odata primite datele respective, sunt manipulate sub forma JSON si salvate pe client. Apoi, se foloseste cheia publica a destinatarului pentru a initializa serviciul de criptare, se cripteaza mesajul cu cheia publica a destinatarului, se seteaza un field de expeditor si se trimite payload-ul criptat catre destinatar.

Dupa ce mesajul este trimis catre destinatar, acesta va fi primit de catre acesta sub forma criptata. Se decripteaza mesajul folosind cheia private a destinatarului si se afiseaza pe ecranul acestuia sub forma de plaintext.



Concluzie

Criptarea de tip end-to-end ofera un grad mai mare de securitate, intrucat doar expeditorul si destinatarul pot accesa continutul mesajelor trimise.

Aplicatia mai poate fi imbunatatita prin diferite procedee menite sa sporeasca securitatea(criptarea cheilor, migrarea schimbului de chei publice direct la client fara ca server-ul sa actionize ca intermediar etc).

Aplicatia mea este o implementare relativ simpla ale unei retele locale de clienti care comunica prin mesaje criptate end-to-end, imitand, la o scara evident mai mica, procedee folosite in aplicatii precum WhatsApp sau Signal.