

Návrh systému pro zabezpečenou komunikaci

PB173 Tematicky zaměřený vývoj aplikací v jazyce C/C++

Matěj Plch, Lukáš Toldy, Maroš Valter

1 Účel systému

Účelem systému je zajistit komunikační platformu odolnou vůči odposlechu třípísmenkovými agenturami. Uživatelé systému mají možnost šifrovaného sdílení souborů a (video)hovorů.

2 Struktura systému

Systém se skládá z jednoho serveru, ke kterému se připojují klienti. Server spravuje seznam klientů a udržuje si přehled, kteří klienti jsou online. Pokud chce některý z klientů zahájit s někým komunikaci, tak si uživatelé přes server vykomunikují podrobnosti o spojení, které je následně realizováno přímo mezi klienty (bez serveru).

3 Šifrování

Komunikace mezi serverem a klienty je šifrována pomocí SSL.

Uživatelé poskytují serveru vlastní veřejný klíč, který mají následně k dispozici ostatní uživatelé. Pokud spolu chtějí uživatelé komunikovat, tak si přes server za pomoci veřejných klíčů vyjednají symetrický šifrovací klíč, který se server nedozví.

4 Případy užití systému a jejich provedení

a) Registrace uživatele

Uživatel pošle serveru svoje ID a veřejný klíč, server zašifruje daným klíčem výzvu a pošle ji klientovi. Pokud se výzva vrátí, tak je registrace úspěšná.

b) Přihlášení do systému

Uživatel pošle serveru svoje ID, server zašifruje výzvu veřejným klíčem uživatele s daným ID a pošle ji klientovi. Pokud se výzva vrátí, tak je přihlášení úspěšné.

c) Ustavení spojení mezi dvěma uživateli

Uživatelé, kteří spolu chtějí komunikovat, si přes server za pomoci dostupných veřejných klíčů šifrovaně vymění informace potřebné pro uskutečnění spojení a symetrický klíč. Každá strana komunikace se podílí na tvorbě poloviny klíče, složením těchto částí vznikne výsledný šifrovací klíč pro dané spojení. Konkrétně oba uživatelé vygenerují náhodných 16 bajtů a pošlou je šifrovaně druhému uživateli, spojením vznikne šifrovací klíč o délce 256 bitů.

5 Funkce serveru

1. registerUser(ID, key)
2. loginUser(ID)
3. logoutUser(ID)
4. deleteUser(ID)
5. sendOnlineUserList(user)
6. resendMessage(user, message)

6 Funkce klienta

1. sendRequest(message)
2. createUserConnection(user, key)
3. sendData(user, data)