Desain Komunikasi Chat

KIJ F

Joshua Kevin Rachmadi 5113100059

Gian Sebastian Anjasmara 5113100132

Rahmat Nazali Salimi 5113100167

1. Metode yang digunakan:
   1. Menggunakan metode enkripsi simetris dengan algoritma RC4 untuk mengamankan isi pesan + digital signaturenya.
   2. Menggunakan hash fuction SHA-512 (menjaga integritas pesan) dan metode enkripsi asimetris dengan algoritma RSA (menjaga keaslian pesan) untuk membuat digital signature dari pesan.
   3. Symmetric key distribution melalui socket. Symmetric key di-generate oleh server, kemudian di-enkripsi menggunakan algoritma RSA dan dikirimkan kepada client hanya pada saat pertama kali socket client terhubung.
   4. Public key distribution menggunakan metode Public Key Directory yang berada pada server.
2. Alur:
   * 1. Server men-generate private key dan public key yang akan digunakan dalam algoritma enkripsi RSA, public key server disimpan dalam bentuk file pada public key directory.
     2. Ketika pertama kali socket client terhubung kepada server:
        1. Client men-generate private key dan public key.
        2. Server mengirimkan suatu penanda unik(dalam program adalah counter) kepada client yang akan digunakan client ketika menyimpan public keynya pada public key directory(membedakan public key client yang satu dengan yang lain).
        3. Server men-generate key simetris (digunakan dalam algoritma enkripsi RC4 (KRC4) ) ketika ada socket client yang terhubung, lalu key tersebut di-enkripsi dengan RSA menggunakan private key milik server
        4. Kemudian hasil enkripsi tersebut dikirimkan kepada client melalui socket yang terhubung, lalu setelah diterima client dilakukan dekripsi menggunakan public key server untuk mendapatkan key RC4
     3. Untuk membuat digital signature dari pesan(memastikan integritas dan keaslian pesan), sebelum dikirim pesan akan dihitung hash valuenya menggunakan algoritma SHA-512, kemudian di-enkripsi hash valuenya menggunakan algoritma RSA
     4. Server dan client saling bertukar pesan yang isi pesannya sekaligus digital signaturenya sudah ter-enkripsi menggunakan algoritma RC4
     5. Ketika client melakukan logout, public key client yang bersangkutan yang tersimpan pada public key directory akan di delete, sehingga public key client tersebut dapat dianggap sebagai session key
3. Login
   1. Client : LOGIN username password

DS = digital signature =

Selanjutnya, pesan dibuat dengan format : message + “ “ + DS, dengan “ “ adalah sebuah spasi yang membedakan DS dengan message

* 1. Server : LOGIN ok/errors

1. Logout
   1. Client : LOGOUT username
   2. Server : LOGOUT ok/error
2. Private message
   1. Client : PM src\_username dest\_username message
3. Create group
   1. Client : CG username group\_name
   2. Server : CG ok/error
4. Group message
   1. Client : GM src\_username group\_name message
5. Broadcast message
   1. Client : BM src\_username message