Dokumen Hasil Diskusi

KIJ D- Aplikasi Chatting



Anggota kelompok:

Fransiskus Dwika 5112100013

Ryan Nathan 5112100079

Brilian T. Nugraha 5112100172

Muh Aunorafiq Musa 5112100209

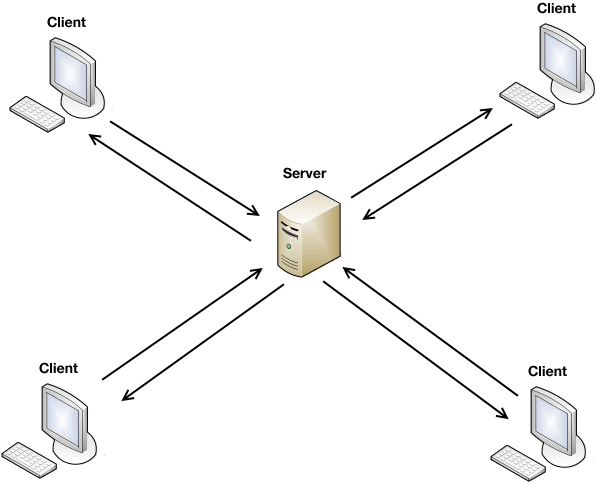
Jurusan Teknik Informatika - Institut Teknologi Sepuluh Nopember

Kampus ITS Keputih Sukolilo Surabaya

2014

Hasil Diskusi

1. Overfiew aplikasi Chatting



* Setiap klien dapat bebas masuk ke dalam jaringan dan menentukan namanya (display name) sendiri
* Setiap klien bebas menentukan klien mana yang akan menerima pesannya
* Server meneruskan pesan dari klien pengirim ke klien penerima
* Pesan tidak di-enkripsi

1. Alur

**Non-secure Chat Protocol**

|  |  |
| --- | --- |
| **Klien** | **Server** |
| 1. Konek ke server, port bebas |  |
|  | 1. Balas dengan: OK\r\n 2. Untuk setiap user lain yang udah konek, kirim ke klien yang baru konek:   !CONNECT <nama\_klien\_lain>\r\n |
| 3. Kirim satu kata\* yg akan jadi display name |  |
|  | 4.a (Kalau nama bisa dipakai), kirim balasan OK\r\n  4.b (Kalau nama tidak bisa dipakai\*\*), kirim balasan NOPE\r\n, balik ke klien tahap no. 3   1. Server mengirim pesan ke semua user lain:   !CONNECT <nama\_yg\_baru\_konek>\r\n |
| 6.a Kirim string dengan format  (nama\_penerima): (isi pesan)\0\*\*\*  6.b Klien menerima pesan dari klien yang lain (melalui server) |  |
|  | 1. Server kirim pesan ke klien penerima dengan format (nama\_pengirim): (isi pesan)\0\*\*\*. |
| 8. Klien diskonek |  |
|  | 1. Server mengirim pesan ke semua user lain:   !DISCONNECT <nama\_yg\_baru\_diskonek>\r\n |

\*panjang nama maksimal 50 karakter tanpa spasi, alphanumeric (a-z,A-Z,0-9)

\*\*nama sudah diambil atau ada karakter yang tidak sesuai

\*\*\*pesan diakhiri dengan null character, panjang pesan maksimal 1000 karakter

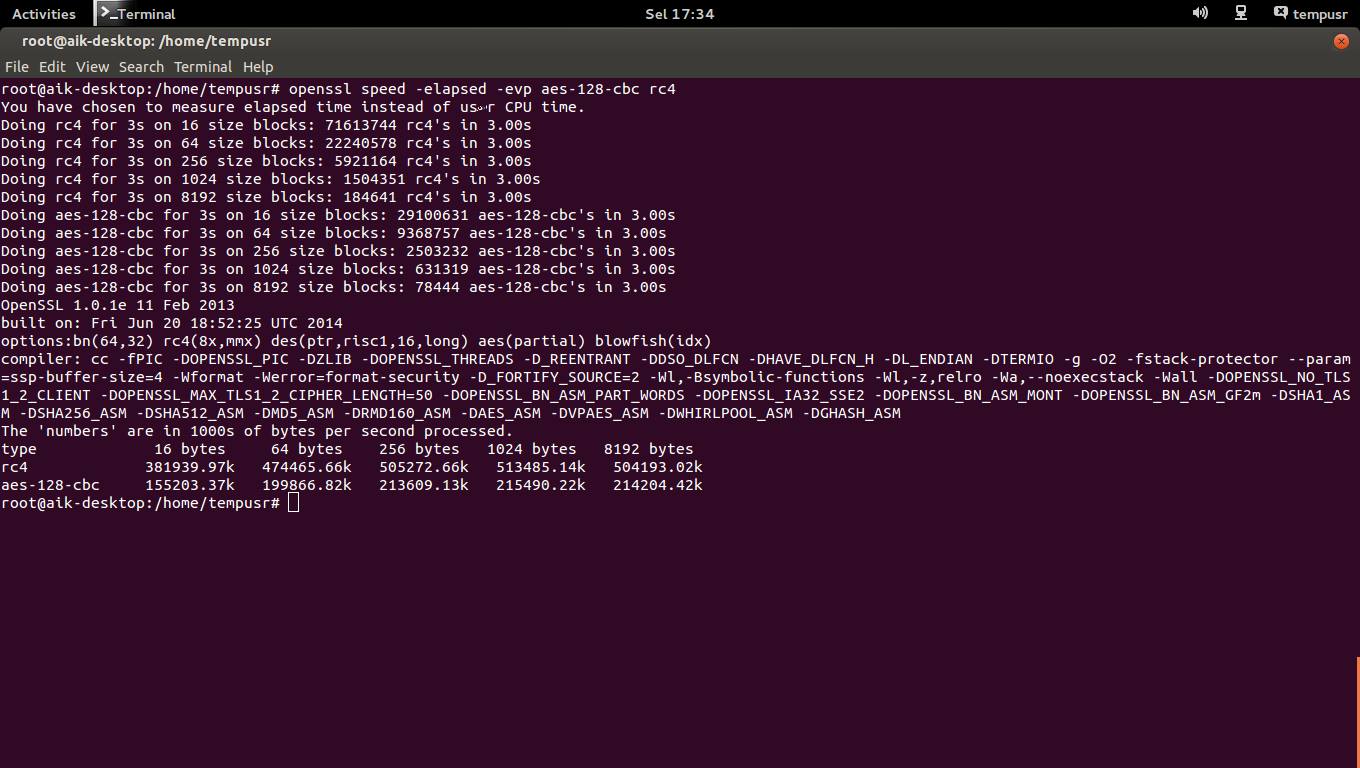
1. Data yang perlu di enkripsi

* String yang dikirim dari klien ke server, maupun sebaliknya.
* Termasuk nama pengirim / penerima

1. Metode Enkripsi yang Digunakan

Metode yang digunakan,yaitu AES:

* + - Runtime enkripsi di komputer baru hampir menyamai runtime enkripsi rc4



* + - Merupakan standar TLS
    - AES di claim merupakan metode enkripsi yang paling aman dibanding DES dan RC4
    - DI cloud computing dan di mobile apps sudah mulai di komersialkan
    - Possible kombinasi untuk brute force attack nya untuk AES 256-bit yaitu 1.1 x
    - Kemungkinan packet loss lebih kecil, ex: jika 1 block loss, maka block selanjutnya nya tidak dapat di decrypt, karena menggunakan key dari blocknya, tetapi block+2 dan seterusnya tetap dapat didecrypt

......

Onerpngifpbgmblvkbmvclbmio[ mgfio [mgbiodfmdfiovmdiovmdfiodfnbdfubndf

afjksdhfhapsofbqgqprgbkjnvjkvnpsdavunsduvisdvuispndvsdpfuinsduvsdanvsain

nfgkjsdfbpiengiergoenofvndfoi

Decrypted possible

Can’t decrypted

Block lost

1. Pengiriman Key

* Menggunakan metode key exchanger: Diffie-Hellman Key Exchange:

1. Metode operasi

* Metode operasi yang dipakai adalah CTR(Counter Mode):
  + Mirip seperti OFB, membuat block cipher bekerja seperti stream cipher, sehingga data yang diproses dapat berupa Byte atau bit, bukan satu blok yang lebih besar seperti mode operasi AES CBC/ECB
  + Runtime nya lebih cepat dari AES CBC, karena data yang diproses tidak masuk ke AES-methodnya, tapi di XOR dengan nilai yang digenerate oleh AES-method dari message sebelumnya
  + width/lebar data yang akan dienkripsi dapat di atur sesuai dengan size block nya, tetapi ingat bahwa kecepatan menurun ketika width semakin kecil didalam rasio lebar data ke ukuran blok .
  + Ketika ada packet loss di block ke x, block yang tidak dapat di decrypt ada 2 block, yaitu block x dan x+1 nya, sehingga tidak memberi efek fatal ke seluruh data yang dikirim
  + Runtime lebih cepat dari rata-rata AES karena enkripsinya dilakukan secara paralel

