Implementasi Algoritma Diffle-Hellman untuk Pertukaran Kunci Sesi Pada *Bluetooth*

Ratna Ekasari Prihandini[1)] - 13504043
[1)] Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika, ITB, Bandung,
email: prihandini.re@google.com

Abstract – *Komunikasi nirkabel makin marak dilakukan seiring dengan perkembangan teknologi dan tuntutan mobilitas yang tinggi. Teknologi nirkabel yang digunakan diantaranya WAP, GPRS, inframerah, dan bluetooth. Saat ini teknologi tersebut telah digunakan baik untuk komunikasi dengan menggunakan PC maupun handphone. WAP dan GPRS biasanya digunakan untuk melakukan akses internet secara langsung dari handphone, sedangkan inframerah dan bluetooth digunakan untuk melakukan koneksi ketika kita membutuhkan dial-up untuk mengakses internet. Seiring dengan perkembangan tren yang ada, bluetooth lebih banyak digunakan untuk komunikasi jarak pendek seperti pengiriman data atau file media antar handphone. Sayangnya penggunaan bluetooth ini sering merugikan pemilik handphone terutama yang tidak memahami faktor keamanan bluetooth. Akibatnya banyak data yang tidak diinginkan bahkan virus yang dapat merusak handphone masuk melalui koneksi tersebut. Untuk itu, diperlukan suatu mekanisme keamanan yang dapat digunakan untuk melakukan autentikasi dan autorisasi pengguna bluetooth. Teknik yang digunakan adalah dengan menggunakan password (kata kunci) atau PIN yang aman dan berbeda-beda untuk tiap koneksi. Permasalahannya adalah bagaimana cara mempertukarkan kata kunci tersebut. Untuk itu, digunakanlah algoritma Diffle-Hellman yang dapat mempertukarkan kunci sesi secara aman untuk digunakan sebelum berkomunikasi.*

Kata Kunci : *Kunci publik, Kunci privat, Diffle-Hellman, Bluetooth*

1. PENDAHULUAN

Pada masa ini *handphone* atau telepon genggam bukan lagi menjadi barang mewah atau kebutuhan sekunder bagi manusia. *Handphone* sudah seperti makanan atau air yang tidak bisa ditinggalkan oleh manusia. Hal ini dikarenakan mobilitas manusia sangat tinggi sehingga kebutuhan komunikasi jarak jauh pun semakin meningkat.

Bentuk komunikasi dan kemudahan yang diinginkan juga beragam dan selalu berubah. Pada awal munculnya teknologi seluler kebutuhan untuk melakukan pembicaraan baik melalui suara maupun teks menjadi fokus pengembangan *handphone.* Suara jernih, sinyal kuat, dan keamanan penggunaan *handphone* terhadap kesehatan merupakan isu yang marak ditawarkan oleh vendor telekomunikasi. Seiring dengan perkembangan teknologi faktor-faktor teknis tersebut berhasil diatasi. Persaingan tidak lagi ada pada keamanan penggunaan yang ditawarkan, melainkan dititikberatkan pada fitur media yang ditawarkan dan kecanggihan sesuai dengan tren kebutuhan yang sedang populer. Sebagai contoh, kebutuhan untuk menyimpan kenangan pada saat kita tidak membawa kamera. Hal ini menyebabkan munculnya *handphone* yang menyediakan kamera didalamnya meski kualitas gambarnya tidak sebagus penggunaan kamera biasa.

Perkembangan teknologi internet juga mempengaruhi perkembangan teknologi telepon genggam. Penggunaan internet untuk melakukan transaksi *real time* memicu perubahan gaya hidup yang sangat signifikan. Pekerjaan apa pun dapat dilakukan dari jarak jauh dengan menggunakan PC atau *notebook* asalkan terkoneksi internet. Kebutuhan ini memicu perkembangan teknologi seluler untuk menyediakan koneksi internet melalui *dial-up*. Teknologi untuk melakukan koneksi antara telepon seluler dan komputer ini diantaranya inframerah (*infrared*) dan *bluetooth*. Untuk melakukan koneksi dengan server provider (*dial-up*) digunakan WAP dan GPRS. WAP biasanya digunakan untuk melakukan streaming langsung dari telepon seluler dengan menggunakan browser yang sudah disediakan.

Inframerah dan *bluetooth* tidak hanya digunakan untuk melakukan koneksi antara komputer dengan *handphone*, tetapi bisa juga antar *handphone* yang sama-sama menyediakan konektivitas melalui inframerah atau *bluetooth*. Perbedaannya adalah jarak dan kecepatan pengiriman data yang dapat dilakukan. Pada koneksi dengan inframerah jarak maksimal yang masih dapat dicapai ± 1 meter, untuk *handphone* biasanya kurang dari 10 cm. Selain itu, arah dari sumber inframerah harus berhadapan dalam satu garis lurus karena inframerah bersifat konvergen satu arah. Akibatnya, koneksi dengan menggunakan inframerah ini kurang disukai. Orang lebih memilih menggunakan *bluetooth* yang memiliki *range* lebih panjang dan tidak harus *real*

point to point. Namun, penggunaan *bluetooth* pada *handphone* seringkali menimbulkan masalah diantaranya masuknya virus *handphone* atau gambar-gambar porno yang tertempel virus *handphone*, yang dapat merusak sistem atau menghapus data-data dari *handphone.*

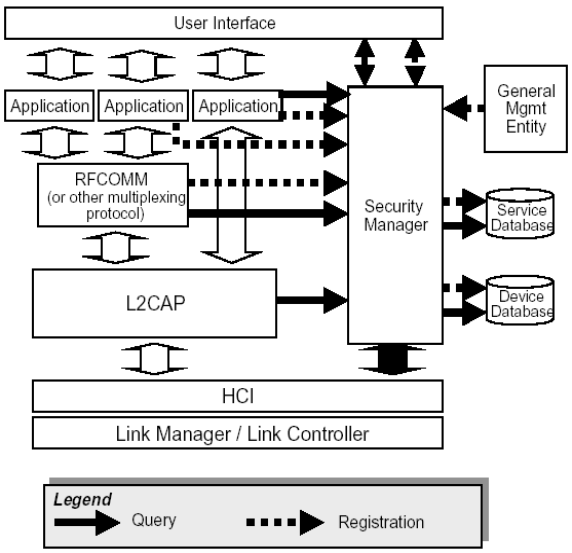
Masalah ini timbul karena pemilik *handphone* biasanya lupa untuk mematikan *bluetooth*nya setelah menggunakannya untuk melakukan koneksi dengan *device* lain. Selain itu, tidak adanya autentikasi dan autorisasi pada saat pengiriman dan penerimaan data pada *handphone* dengan menggunakan *bluetooth* mengakibatkan data apapun yang terpancar dapat diterima oleh *handphone* kita. Berbeda dengan komputer atau *notebook* yang telah dilengkapi aplikasi atau fungsi untuk melakukan autorisasi dan autentifikasi sebelum melakukan pertukaran data. Untuk itu, pada makalah ini akan dibahas mengenai penggunaan algoritma diffle helman untuk melakukan pertukaran kunci pada koneksi *bluetooth* sebelum melakukan pertukaran data.

2. DASAR TEORI

2.1 *Bluetooth* dan Arsitekturnya

Bluetooth merupakan teknologi sambungan nirkabel jarak pendek. Biasanya digunakan untuk pengiriman data dalam ukuran kecil antar perangkat elektronik. Dapat digunakan untuk melakukan sambungan antara perangkat komputer dengan telepon atau antar telepon dengan jarak sambungan bervariasi bergantung pada jenis pemancarnya.

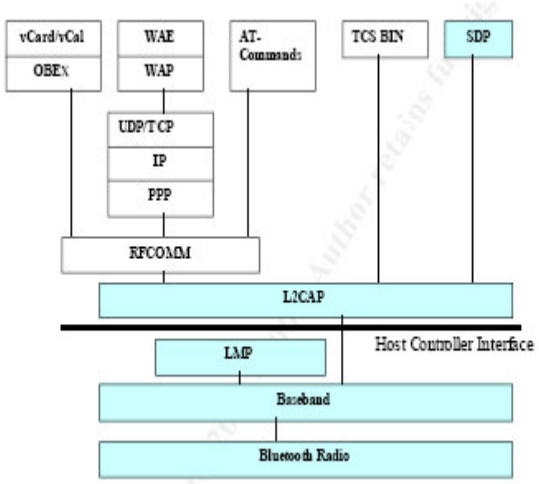
Arsitektur dari *bluetooth* dapat dilihat pada Gambar 1



Gambar 1 : Arsitektur Bluetooth

Pada arsitektur *bluetooth* terdapat beberapa layer protokol yaitu layer data link dan *application* serta sebuah *security manager* yang digunakan untuk menyimpan informasi terkait keamanan transmisi pada *bluetooth*.

Susunan protokol pada *bluetooth* dapat dilihat pada Gambar 2



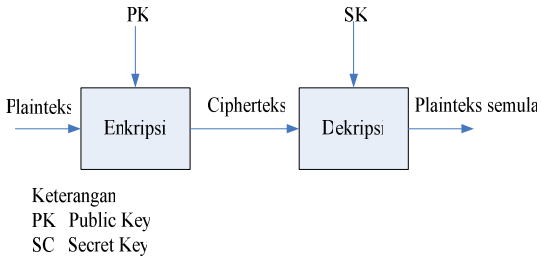
Gambar 2 Layer Protokol Bluetooth

Bluetooth menyediakan layanan protokol baik TCP/IP maupun UDP. *Bluetooth* mendukung untuk melakukan pengiriman hasil enkripsi sebesar 128 bit. Arsitektur yang digunakan FHSS @ 1600 hop/s.

2.2 Algoritma Kriptografi Kunci Privat dan Publik

Algoritma kunci publik dan privat ditemukan oleh James H. Ellis, Clifford Cocks, dan Malcolm Williamson di Inggris pada awal 1970. Sayangnya algoritma tersebut tidak dipublikasikan hingga pada tahun 1976 whitfield Diffie dan Martin Hellman mempublikasikan makalah yang membahas tentang distribusi kunci rahasia pada saluran pada komunikasi publik yang tidak aman dengan menggunakan metode pertukaran kunci yang belakangan dikenal dengan nama algoritma pertukaran kunci Diffle-Helman.

Konsep utama dari algoritma kunci privat dan publik adalah adanya perbedaan kunci yang digunakan untuk melakukan enkripsi dan dekripsi. Kunci publik digunakan untuk melakukan enkripsi dan kunci privat digunakan untuk melakukan dekripsi. Prosesnya dapat dilihat pada Gambar 3



Gambar 3 : Proses pada Algoritma Kunci Publik

Kelebihan dari penggunaan kunci publik ini diantaranya:
a. Hanya kunci privat yang perlu dijaga kerahasiannya akan tetapi autentifikasi kunci publik harus tetap terjamin. Tidak ada kebutuhan mengirim kunci privat sebagaimana pada sistem kriptografi simetri.
b. Pasangan kunci publik dan privat tidak perlu diubah bahkan dalam periode lama
c. Dapat digunakan untuk melakukan pengamanan kunci simetri
d. Beberapa dapat dilakukan untuk melakukan penanda tanganan digital.

Adapun kelemahan dari penggunaan kunci privat dan publik ini diantaranya :
a. Enkripsi dan dekripsi lebih lambat
b. Ukuran cipherteks lebih besar dari plainteks

Aplikasi dari kriptografi kunci privat dan publik dibagi dalam tiga kategori yaitu :
a. Kerahasiaan data
   Seperti pada algoritma kriptografi simetri, kunci publik dan privat dapat dilakukan untuk melakukan enkripsi dan dekripsi. Contoh algortimanya RSA, knapsack, Rabin, ElGamal, dan Elliptic Curve Cryptography (ECC).
b. Tanda tangan digital
   Merupakan aplikasi untuk membuktikan autentikasi pesan maupun pengirimnya, contoh algoritmanya RSA, DSA, dan ElGamal.
c. Pertukaran kunci (*key exchange*)
   Algortima kunci publik digunakan untuk melakukan pertukaran kunci simetri, contoh algortimanya RSA dan Diffle-Helman

2.3 Algoritma Diffle-Helman

Algoritma Diffle-Helman digunakan untuk melakukan pertukaran kunci sesi untuk melakukan komunikasi antara dua orang atau lebih. Kekuatan algoritma ini terletak pada sulitnya menghitung logaritma diskrit.

Sebelum melakukan komunikasi kedua pihak menyepakati dua buah bilangan prima besar yaitu n dan g sedemikian sehingga $g < n$. Nilai n dan g tidak perlu dirahasiakan. Bahkan pihak A dan B dapat membicarakannya melalui saluran yang tidak aman sekalipun.

Algoritma Diffle-Helman adalah sebagai berikut :
a. Pihak A membangkitkan bilangan bulat acak yang besarnya x dan mengirimkan hasil perhitungan berikut kepada pihak B :
   $$X = g^x \bmod n \quad (1)$$
b. Pihak B membnagkitkan bilangan bulat acak besarnya y dan mengirimkan perhitungan berikut kepada pihak A:
   $$Y = g^y \bmod n \quad (2)$$
c. Pihak A menghitung :
   $$K = Y^x \bmod n \quad (3)$$
d. Pihak B menghitung :
   $$K' = X^y \bmod n \quad (4)$$
   Jika perhitungan dilakukan dengan benar maka :
   $$K = K' \quad (5)$$
   Ini berarti kunci simetri sudah berhasil diterima oleh kedua pihak. Baik K dan K' sama dengan :
   $$g^{xy} \bmod n \quad (6)$$

Pihak C yang menyadap pembicaraan tidak akan mengetahui K. Ia hanya memiliki informasi n, g, X, dan Y tetapi tidak memiliki x dan y. Untuk mengetahui membutuhkan perhitungan logaritma diskrit yang sangat sulit dikerjakan.

3. DIFFLE-HELMAN PADA *BLUETOOTH*

Sistem keamanan pada *bluetooth* dirancang secara berpasangan yaitu pada setiap perangkat autentifikasi dan enkripsi dilakukan dengan cara yang sama. *Bluetooth* memiliki beberapa tingkat keamanan yang berbeda yang dapat didefinisikan untuk berbagai perangkat dan layanan. Setiap perangkat mendapat status saat perangkat tersebut untuk pertama kali terhubung dengan perangkat lain.

Tingkat keamanan *bluetooth* yaitu sebagai berikut :
a. *Non Secure*, perangkat tidak akan menginisialisasi keamanan
b. *Service Level Security,* perangkat tidak menginisialisasi keamanan sebelum kanal terhubung pada level L2CAP*(Logical Link Control and Adaptaion Layer Protocol)* atau perangkat telah dinyatakan sebagai perangkat yang *trusted*.
c. *Link Security,* perangkat tidak melakukan prosedur keamanan sebelum keamanan pada tingkat LPM(*Link Manager Protocol*) selesai dibangun.

Sebelum melakukan sambungan *bluetooth* melakukan autorisasi dan autentifikasi perangkat. Autentikasi merupakan proses verifikasi pihak lain pada koneksi. Autentikasi dilakukan berdasarkan kunci sambungan atau dengan pencocokan nomor PIN. Autorisasi merupakan proses yang akan menentukan apakah suatu perangkat lunak A diijinkan untuk melakukan akses layanan terhadap B. Pada tahap ini *bluetooth* menggunakan keamanan tingkat sambungan dimana setiap koneksi diberikan kunci autentifikasi unik rahasia dan kunci enkripsi yang diturunkan dari autentifikasi.

Perangkat dapat memiliki dua tingkat kepercayaan *(trust)* , terpercaya (*trusted)* dan tidak terpecaya (*untrusted)*. Tingkat *trusted* membutuhkan hubungan yang tetap dan terpercaya serta memiliki akses ke semua layanan. Perangkat harus diautentifikasi terlebih dahulu. Perangkat dengan status *untrusted* tidak memiliki hubungan yang tetap dan akses layanannya terbatas. Perangkat *untrusted* dapat juga memiliki hubungan yang tetap tetapi tidak dikenali sebagai *trusted*. Perangkat yang baru terhubung ditandai sebagai perangkat tidak dikenal dan selalu *untrusted*.

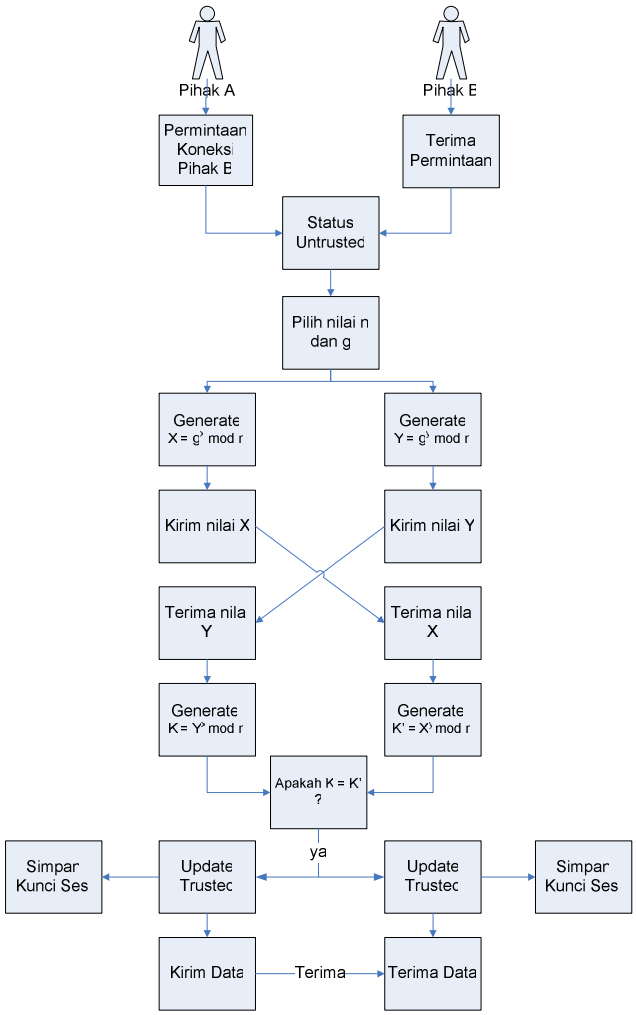
Dengan demikian, keamanan utama pada *bluetooth* terletak pada layer data link atau *link security* yaitu untuk melakukan pertukaran kunci sesi (*session key*) yang nantinya akan digunakan sebagai kunci untuk menurunkan kunci apabila data yang akan ditransfer memerlukan enkripsi. Salah satu algoritma yang dapat digunakan untuk melakukan pertukaran kunci ini adalah Diffle-helman.

Terdapat empat data penting dalam penggunaan algoritma ini, yaitu : alamat perangkat, kunci privat untuk melakukan sambungan, kunci privat untuk melakukan enkripsi, dan bilangan random yang dibangkitkan berbeda-beda untuk tiap koneksi ke perangkat yang berbeda.

Alamat perangkat biasanya didapatkan pada saat melakukan permintaan koneksi atau melakukan monitoring terhadap permintaan koneksi. Kunci privat untuk melakukan sambungan akan di*generate* menggunakan algortima diffle hellman. Kunci untuk melakukan enkripsi di*generate* dari kunci privat. Bilangan random yang akan digunakan sebagai faktor pemangkatan di*generate* secara otomatis menggunakan random generator yang dipilih oleh implementor. Pemilihan teknik untuk melakukan *generate* bilangan random ini akan semakin memperkuat kekuatan algoritma Diffle hellman yang digunakan.

Untuk algoritma autentikasi ukuran kunci selalu 128 bits sedangkan untuk algoritma enkripsi ukuran kunci bervariasi antara 1 hingga 16 oktet (8-128 bits). Ukuran kunci enkripsi dapat diubah karena dua alasan. Pertama karena adanya aturan mengenai kriptografi yang berbeda di tiap Negara. Alasan kedua adalah untuk memfasilitasi kemungkinan meng-upgrade sistem keamanan tanpa mendesain ulang perangkat keras enkripsi.

Proses penggunaan algoritma kunci ini dapat dilihat pada Gambar 4



Gambar 4 : Mekanisme Penggunaan Diffle-Hellman

Jika data membutuhkan enkripsi pihak A akan memilih mode enkripsi, sistem akan melakukan *generate* kunci untuk melakukan enkripsi dan melakukan enkripsi terhadap data yang akan dikirim. Pada saat diterima oleh pihak B, akan dilakukan proses dekripsi dengan menggunakan kunci yang sama. Karena kunci untuk dekripsi diturunkan dari kunci sesi yang sama dengan kunci sesi pihak A.

Terdapat tiga mode enkripsi dari pesan yang dipancarkan berdasar baseband:

a. Tanpa enkripsi
   Setting default, tidak ada pesan dienkripsi.
b. Enkripsi titik ke titik.
   Pesan yang dipancarkan tidak dienkripsi. Enkripsi ini dapat diaktifkan pada saat prosedur pembentukan hubungan atau setelah hubungan terbentuk.
c. Enkripsi titik ke titik (peer-to-peer) dan pancaran (broadcast).
   Semua pesan dienkripsikan. Enkripsi dapat dilakukan hanya setelah koneksi terbentuk. Setting ini tidak aktif kecuali semua sambungan yang terpengaruh memiliki kunci sambungan master yang sama

Pseudo-code dari penggunaan algoritma Diffle-Helman ini adalah sebagai berikut:

a. Pihak yang melakukan permintaan koneksi

```
Create_Connection
If Connected then
    UpdateStateUntrusted
    Read(n)
    Read(g)
    BigInt  X = g^x mod n
    Send(X)

    While monitoring do
    Read(Y)
    BigInt K = Y^x mod n
    If Save=True then
            UpdateStateTrusted
            SaveKey (K)
            If send = true then
                    Send(Data)
                    If Close = true then
                            Close_Connection

    Else
    Close_Connection
Else
    Write("Connection Failed")
```

b. Pihak yang menerima koneksi

```
While monitoring do
    Receive_Connection
    If Connected then
        UpdateStateUntrusted
        Read(n)
        Read(g)
        BigInt  Y = g^y mod n
        Send(Y)

While monitoring do
    Read(X)
    BigInt K'= X^y mod n
    If Save=True then
        UpdateStateTrusted
        SaveKey (K')
        If receive = true then
            Receive(Data)
            If Close = true then
                    Close_Connection
Else
    Close_Connection
Else
    Write("Connection Failed")
```

Penggunaan mekanisme ini akan membatasi adanya pengiriman data yang tidak diinginkan. Hal ini dikarenakan hanya perangkat dengan status *trusted* saja yang dapat melakukan pengiriman data. Perangkat yang termonitor dan tertangkap sinyal *bluetooth*nya meskipun statusnya terkoneksi tetap tidak dapat mengirimkan data sampai statusnya *trusted*.

4. KESIMPULAN

Dari pembahasan mengenai keamanan dengan menggunakan *bluetooth* dapat diambil kesimpulan sebagai berikut :

a. Tingkat keamanan komunikasi data dengan menggunakan *bluetooth* terutama terletak pada layer data link
b. Keamanan pada komunikasi data menggunakan *bluetooth* ditentukan kunci sesi yang digunakan
c. Dibutuhkan suatu mekanisme pertukaran kunci sesi yang aman untuk melakukan koneksi dengan *bluetooth*
d. Algoritma Diffle-Hellman dapat digunakan untuk melakukan pertukaran kunci sesi pada komunikasi *bluetooth*
e. Enkripsi dapat dilakukan dengan menggunakan algoritma lain dengan kunci sesi sebagai *seed* untuk melakukan *generate* kunci yang akan digunakan untuk enkripsi dan dekripsi
f. Algoritma lain juga dapat digunakan untuk melakukan pertukaran kunci asalkan panjang kunci yang dapat dikirimkan sepanjang 128 bit.

5. REFERENSI

[1] Munir, Rinaldi. *Diktat Kuliah IF5054 Kriptografi.*Departemen Informatika ITB. 2005

[2] *Specification of the Bluetooth System*, version 1.2, 5 November 2003.

[3] Muller, Thomas *Bluetooth WHITE PAPER: Bluetooth Security Architecture,* Version 1.0, 15 July 1999