Penerapan Otentikasi Kunci Publik pada SSH menggunakan Kriptografi Kunci Publik

Angela Lynn - 13513032
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
angel_lynz95@hotmail.com

***Abstrak*—Makalah ini berisi penjelasan mengenai penerapan otentikasi kunci publik pada SSH menggunakan kriptografi kunci publik dan perbandingannya dengan otentikasi kata sandi. Pada otentikasi kunci publik, pengguna harus membangkitkan sepasang kunci, yaitu kunci publik dan kunci privat. Kunci privat digunakan untuk membangkitkan *signature*, sedangkan kunci publik digunakan untuk melakukan verifikasi *signature* tersebut. Setelah melakukan percobaan dan dianalisis, dapat disimpulkan bahwa otentikasi kunci publik lebih aman dan fleksibel dibandingkan otentikasi kata sandi.**

Kata Kunci—kriptografi; kunci publik; kunci privat; ssh; otentikasi

I. PENDAHULUAN

Saat akan melakukan *login* ke suatu server, otentikasi sangat diperlukan untuk mengidentifikasi pengguna yang berhak mengakses server tersebut. Secara umum, orang-orang akan menggunakan otentikasi kata sandi. Namun otentikasi ini memiliki kelemahan. Apabila ada orang yang berhasil menyerang server tersebut, maka orang tersebut bisa mempelajari kata sandi yang digunakan.

Permasalahan ini bisa ditangani dengan tipe otentikasi yang lain, yaitu otentikasi kunci publik. Sesuai dengan namanya, otentikasi ini menerapkan kriptografi kunci publik. Oleh karena itu, pada makalah ini akan dibahas mengenai penerapan otentikasi kunci publik meggunakan SSH untuk membuktikan bahwa otentikasi ini lebih baik dibandingkan otentikasi kata sandi.

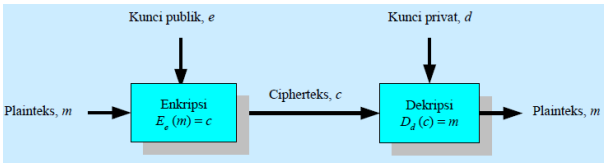
II. TEORI DASAR

A. *Kriptografi Kunci Publik*

Sampai akhir tahun 1970, hanya ada sistem kriptografi kunci-simetri. Permasalahan timbul disini, yaitu bagaimana caranya mengirimkan kunci rahasia kepada penerima. Kunci rahasia harus dikirim melalui saluran yang benar-benar aman. Namun saluran jenis ini umumnya lambat dan mahal. Oleh karena itu, muncullah ide kriptografi kunci publik.

Pada kriptografi kunci publik, masing-masing pengirim dan penerima mempunyai sepasang kunci:

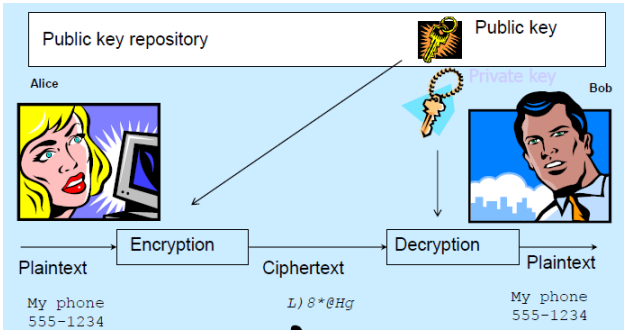
1. Kunci publik: untuk mengenkripsi pesan
2. Kunci privat: untuk mendekripsi pesan



Gambar 1 Enkripsi-Dekripsi Kunci Publik dan Kunci Privat

Berikut merupakan langkah-langkah kriptografi kunci publik secara umum.

1. Misalkan pengirim pesan adalah A dan penerima pesan adalah B.
2. A mengenkripsi pesan dengan kunci public B.
3. B mendekripsi pesan dengan kunci privatnya sendiri.



Gambar 2 Kriptografi Kunci Publik

Keuntungan kriptografi kunci publik:

1. Tidak diperlukan pengiriman kunci rahasia.
2. Jumlah kunci dapat ditekan..

Kriptografi kunci publik didasarkan pada fakta:

1. Komputasi untuk enkripsi/dekripsi pesan mudah dilakukan.
2. Secara komputasi hampir tidak mungkin menurunkan kunci privat, bila diketahui kunci publik.

Pembangkitan sepasang kunci pada kriptografi kunci publik didasarkan pada persoalan integer klasik sebagai berikut:

1. Pemfaktoran

   Diberikan bilangan bulat n. Faktorkan n menjadi faktor-faktor primanya. Semakin besar n, semakin sulit memfaktorkan. Algoritma yang menggunakan prinsip ini adalah Rivest-Shamir-Adleman (RSA).

2. Logaritma Diskrit

   Temukan x sedemikian sehingga $a^x \equiv b \pmod n$. Perhitungan ini sulit dihitung. Algoritma yang menggunakan prinsip ini adalah ElGamal dan *Digital Signature Algorithm* (DSA).

3. *Elliptic Curve Discrete Logarithm Problem* (ECDLP)

   Diberikan P dan Q adalah dua buah titik di kurva eliptik, carilah integer n sedemikian sehingga P = nQ. Algoritma yang menggunakan prinsip ini adalah *Elliptic Curve Cryptography* (ECC).

B. *Otentikasi Kunci Publik*

Otentikasi kunci publik adalah salah satu alternatif, selain otentikasi kata sandi, yang digunakan untuk mengidentifikasi pihak yang berhak untuk mengakses suatu server. Pada otentikasi kata sandi, pengguna harus memasukkan kata sandi yang tepat supaya bisa mengakses server. Berbeda dengan otentikasi kunci publik.

Pada otentikasi kunci publik, pengguna harus membangkitkan sepasang kunci, yaitu kunci publik dan kunci privat. Kunci privat ini akan digunakan untuk membangkitkan *signature*. Kemudian kunci publik pasangannya akan digunakan untuk melakukan verifikasi *signature* tersebut.

Berikut merupakan langkah-langkah otentikasi kunci publik secara umum.

1. Membangkitkan sepasang kunci, yaitu kunci publik dan kunci privat.
2. Kunci publik disimpan di server, sedangkan kunci privat disimpan untuk diri sendiri.
3. Saat melakukan *login* ke server, bangkitkan *signature* dengan kunci privat. Server akan melakukan verifikasi dengan kunci publik yang tersimpan di server.

C. *SSH*

Secure Shell (SSH) adalah protokol jaringan terenkripsi yang beroperasi pada layer ke tujuh di OSI model. SSH menggunakan kriptografi kunci publik untuk melakukan otentikasi pada *remote computer* dan penggunanya.

Berikut merupakan beberapa cara untuk menggunakan SSH.

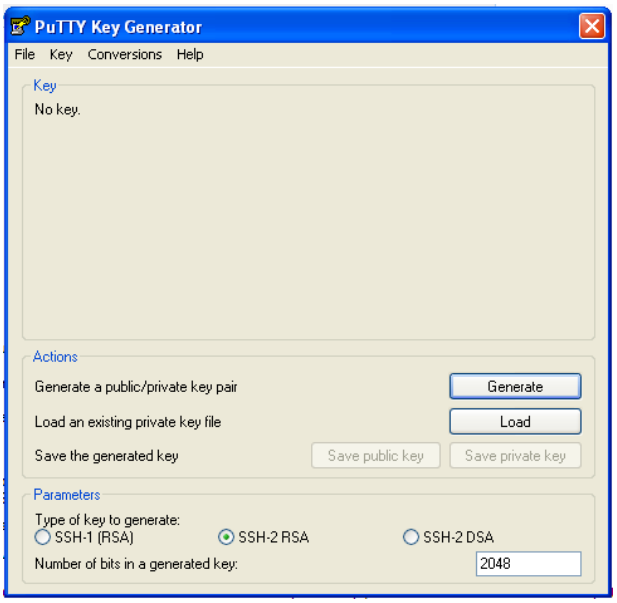
1. Membangkitkan kunci publik dan kunci privat secara otomatis untuk enkripsi koneksi jaringan. Kemudian menggunakan otentikasi kata sandi saat *login*.
2. Membangkitkan kunci publik dank unci privat secara manual, sehingga otentikasi yang digunakan saat *login* adalah otentikasi kunci publik.

III. Otentikasi Kunci Publik pada SSH

Pada bagian ini, akan dijelaskan bagaimana melakukan otentikasi kunci publik pada SSH. Adapun *tool* yang akan digunakan adalah PuTTY dan PuTTYgen. PuTTY digunakan untuk membantu proses otentikasi, sedangkan PuTTYgen digunakan untuk membangkitkan kunci publik dan kunci privat yang akan digunakan PuTTY.

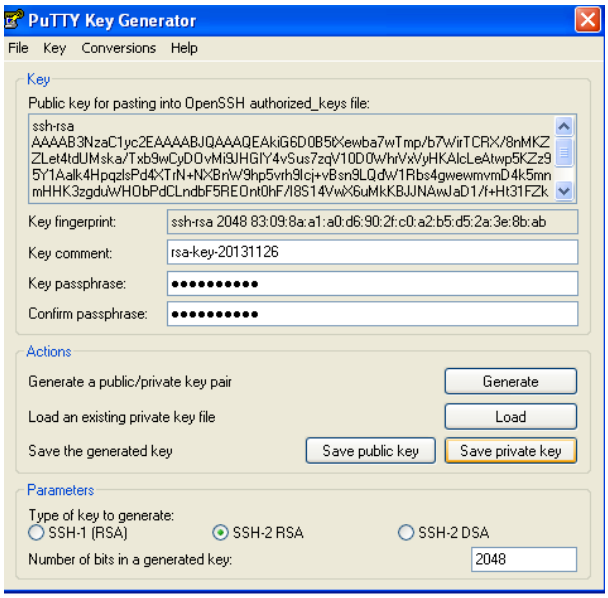
Sebelum melakukan otentikasi, perlu membangkitkan kunci publik dan kunci privat terlebih dahulu. Berikut merupakan langkah-langkahnya, menggunakan PuTTYgen.

1. Pilih jenis kunci yang ingin dibangkitkan. Ada tiga tipe, yaitu:
   a. Kunci RSA dengan protokol SSH 1
   b. Kunci RSA dengan protokol SSH 2
   c. Kunci DSA dengan protokol SSH 2
2. Pilih ukuran (kekuatan) kunci. Ukuran yang biasa digunakan adalah 2048 bit.
3. Pilih tombol ‘Generate’ untuk membangkitkan kunci.



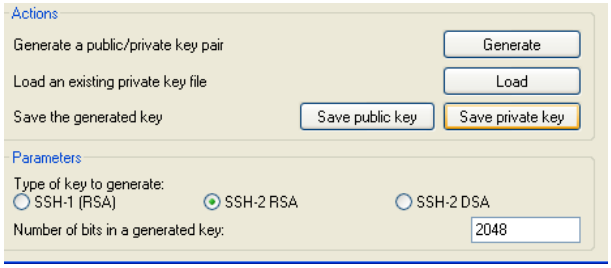
Gambar 3 Pembangkitan Kunci

4. Lakukan konfigurasi *passphrase* untuk kunci yang sudah dibangkitkan. *Passphrase* ini digunakan untuk enkripsi kunci saat disimpan di komputer.



Gambar 4 Konfigurasi Passphrase

5. Pilih ‘Save private key’ untuk menyimpan kunci privat pada direktori tertentu.
6. Pilih ‘Save public key’ untuk menyimpan kunci publik pada direktori tertentu.



Gambar 5 Simpan Kunci

Berikut merupakan cara untuk konfigurasi supaya server menerima otentikasi kunci publik.

- Gunakan PuTTY untuk terhubung dengan server SSH.
- Saat ini server masih melakukan otentikasi kata sandi. Oleh karena itu, *login* dengan *username* dan kata sandi.
- Jika server menggunakan protokol SSH 1, masuk ke direktori .ssh dan buat atau buka *file* authorized_keys. Kemudian *copy* semua teks dari *file* kunci publik yang sudah disimpan sebelumnya, masukkan ke *file* authorized_keys tersebut dan simpan.
- Jika server menggunakan OpenSSH protokol SSH 2, caranya sama seperti di atas, hanya saja nama filenya adalah authorized_keys2.
- Jika server menggunakan *software* SSH lain, ikuti prosedur sesuai dengan *software* tersebut.
- Saat ini server sudah menerima otentikasi kunci publik.

Setelah konfigurasi dilakukan, maka server pun bisa melakukan otentikasi kunci publik. Berikut langkah-langkahnya:

1. Pilih *file* kunci privat yang sudah disimpan di direktori, untuk dimasukkan ke PuTTY.
2. PuTTY akan membangkitkan *signature* menggunakan kunci privat tersebut.
3. *Signature* yang dibangkitkan akan digunakan oleh server untuk diverifikasi dengan kunci publik yang sudah tersimpan di server.

IV. Analisis

Berdasarkan percobaan pada bagian III, saya pun mendapatkan pengetahuan mengenai otentikasi kunci publik dan kelebihan serta kekurangannya dibandingkan dengan otentikasi kata sandi.

Kelebihan otentikasi kunci publik dibandingkan otentikasi kata sandi:

- Lebih aman, karena menggunakan kriptografi kunci publik. Jika ada yang berhasil menyerang server, penyerang tersebut tidak akan bisa mendapat informasi kunci privat, karena di server hanya tersimpan kunci publik.
- Lebih fleksibel, karena tidak perlu memasukkan kata sandi saat *login*.

Kekurangan otentikasi kunci publik dibandingkan otentikasi kata sandi:

- Konfigurasinya yang cukup rumit.
- Kunci privat harus disimpan di komputer dengan kondisi yang benar-benar aman. Oleh karena itu, biasanya kunci privat dienkripsi terlebih dahulu sebelum disimpan.

V. Kesimpulan

Berdasarkan ilmu dan pengetahuan yang penulis dapatkan dari percobaan dan referensi-referensi yang digunakan untuk menyelesaikan makalah ini, penulis menarik kesimpulan bahwa:

1. Terdapat dua jenis otentikasi, yaitu otentikasi kata sandi dan otentikasi kunci publik.
2. Otentikasi kunci publik lebih aman dan fleksibel dibandingkan otentikasi kata sandi.
3. Otentikasi kunci publik bisa diterapkan pada SSH, menggunakan kriptografi kunci publik.

VI. Ungkapan Terima Kasih

Penulis memanjatkan syukur kepada Tuhan Yang Maha Esa. Atas berkat dan rahmat-Nya, penulis dapat menyelesaikan makalah ini dengan baik. Penulis mengucapkan terima kasih kepada dosen IF4020 Kriptografi, yaitu Bapak Rinaldi Munir atas ilmu dan didikan yang diberikan oleh beliau, sehingga penulis bisa mendapatkan inspirasi selama pembuatan makalah. Penulis juga mengucapkan terima kasih kepada semua pihak yang sudah membantu penulis memberikan ide dalam pengerjaan makalah ini, baik secara langsung maupun tidak langsung.

Pernyataan

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 19 Mei 2016

Angela Lynn – 13513032

Referensi

[1] Munir, Rinaldi, "Kriptografi Kunci-Publik (2015)".

[2] http://the.earth.li/~sgtatham/putty/0.55/htmldoc/Chapter8.html, diakses pada tanggal 16 Mei 2016 pukul 17.53.

[3] https://www.linode.com/docs/security/use-public-key-authentication-with-ssh, diakses pada tanggal 17 Mei 2016 pukul 11.05.