SSH (SECURE SHELL) DAN SSL (SECURE SOCKET LAYER)

Oleh : La Ode Abdul Jumar

I. PENDAHULUAN

Perkembangan Internet yang cukup pesat membawa pengaruh yang cukup besar bagi pihak-pihak yang memanfaatkan internet ini untuk melakukan berbagai hal misalnya tukar-menukar data, transaksi online, promosi dan lain-lain. Seiring dengan kemajuan tersebut kebutuhan akan keamanan dan kelancaran dalam berinternet sangat diperlukan karena kemajuan teknologi internet berbanding lurus dengan kejahatan-kejahatan yang ada dalam internet itu sendiri.

Dengan adanya kejahatan-kejahatan internet ini para pengguna semakin tidak aman dan menjadi intaian para penjahat setiap kali mereka berinternet, maka diperlukan solusi yang bisa membatu agar data yang dipertukarkan bisa aman dan bisa sampai ketujuan sesuai dengan yang diinginkan. Salah satu solusi yang ditawarkan adalah dengan menggunakan metode enkripsi yaitu suatu metode yang digunakan untuk mengamankan data dengan mengubah data asli kedalam bentuk unicode dengan aturan tertentu. Ada beberapa metode enkripsi yang bisa digunakan diantaranya adalah dengan metode *secure shell (*SSH*) dan Secure Socket Layer* (SSL).

II. METODE PENULISAN

Dalam penulisan makalah ini dalam pengambilan datanya digunakan metode :

1. Studi literatur/artikel dari internet
2. Studi litertur dari majalah Neotek

III. PEMBAHASAN

1. Pengertian SSH (Secure Shell) dan SSL (Secure Socket Layer)

Pada awalnya SSH dikembangkan oleh Tatu Yl nen di Helsinki University of Technology. SSH memberikan alternatif yang secure terhadap remote session tradisional dan file transfer protocol seperti telnet dan relogin.Protokol SSH mendukung otentikasi terhadap remote host, yang dengan demikian meminimalkan ancaman pemalsuan identitas client lewat IP address spoofing maupun manipulasi DNS. Selain itu SSH mendukung beberapa protokol enkripsi secret key (DES,TripleDES,IDEA, dan Blowfish) untuk membantu memastikan privacy dari keseluruhan komunikasi, yang dimulai dengan username/password awal.SSH menyediakan suatu virtual private connection pada application layer, mencakup interactive logon protocol (ssh dan sshd) serta fasilitas untuk secure transfer file (scd). Setelah meng-instal SSH, sangat dianjurkan untuk mendisable telnet dan rlogin. Implementasi SSH pada linux diantaranya adalah OpenSSH.

SSH merupakan paket program yang digunakan sebagai pengganti yang aman untuk rlogin, rsh dan rcp. Ia menggunakan public-key cryptography untuk mengenkripsi komunikasi antara dua host, demikian pula untuk autentikasi pemakai. Ia dapat digunakan untuk login secara aman ke remote host atau menyalin data antar host, sementara mencegah man-in-the-middle attacks (pembajakan sesi) dan DNS spoofing atau dapat dikatakan Secure Shell adalah program yang melakukan loging terhadap komputer lain dalam jaringan, mengeksekusi perintah lewat mesin secara remote, dan memindahkan file dari satu mesin ke mesin lainnya.

SSL (Secure Socket Layer) dikembangkan oleh Netscape untuk mengamankan HTTP dan sampai sekarang masih inilah pemanfaatan utama SSL. SSL menjadi penting karena beberapa produk umum seperti Netscape Communicator, Internet Explorer, dan WS_FTP Pro, yang merupakan produk yang lazim digunakan, menggunakan SSL. Secure Sockets Layer, adalah metode enkripsi yang dikembangkan oleh Netscape untuk memberikan keamanan di Internet. Ia mendukung beberapa protokol enkripsi dan memberikan autentikasi client dan server. SSL beroperasi pada layer transpor, menciptakan saluran enkripsi yang aman untuk data, dan dapat mengenkripsi banyak tipe data. Hal ini dapat dilihat ketika mengunjungi site yang aman untuk melihat dokumen online aman dengan Communicator, dan berfungsi sebagai dasar komunikasi yang aman dengan Communicator, juga dengan enkripsi data Netscape Communication lainnya. Atau dapat dikatakan bahwa SSL merupakan Protokol berlapis. Dalam tiap lapisannya, sebuah data terdiri dari panjang, deskripsi dan isi. SSL mengambil data untuk dikirimkan, dipecahkan kedalam blok-blok yang teratur, kemudian dikompres jika perlu, menerapkan MAC, dienkripsi, dan hasilnya dikirimkan. Di tempat tujuan, data didekripsi, verifikasi, dekompres, dan disusun kembali. Hasilnya dikirimkan ke klien di atasnya

Kegunaan SSH dan SSL

SSL dirancang untuk mengamankan sesi web, sedangkan SSH dirancang untuk menggantikan protokol telnet dan FTP. Keduanya mempunyai banyak fitur lain, tetapi tujuan utamanya memang untuk mengamankan komunikasi melalui internet.

SSL telah digunakan untuk mengamankan protokol-protokol yang insecure menjadi secure. SSL menjadi perantara antara pemakai dengan protokol HTTP dan menampilkan HTTPS kepada pemakai. Hal yang sama dapat dilakukan pula terhadap protokol-protokol insecure lain seperti POP3, SMTP, IMAP dan apasaja yang merupakan aplikasi TCP.

Adapun SSH merupakan produk serbaguna yang dirancang untuk melakukan banyak hal, yang kebanyakan berupa penciptaan tunnel antar host. Beberapa implementasi SSH tergantung pada SSL libraris karena SSH dan SSL menggunakan banyak menggunakan algoritma enkripsi yang sama (misalnya TripleDES(Pengembangan dari DES oleh IBM).), Algoritma enkripsi lain yang didukung oleh SSH di antaranya *BlowFish* (BRUCE SCHNEIER), *IDEA (The International Data Encryption Algorithm)*, dan *RSA (The Rivest-Shamir-Adelman)*. Dengan berbagai metode enkripsi yang didukung oleh SSH, Algoritma yang digunakan dapat diganti secara cepat jika salah satu algoritma yang diterapkan mengalami gangguan.

SSH tidak berdasarkan SSL seperti halnya HTTPS berdasarkan SSL. SSH mempunyai jauh lebih banyak kelebihan daripada SSL, dan keduanya tidak berhubungan satu sama lain.

Keduanya merupakan dua protokol yang berbeda, namun dalam mencapai tujuan-tujuannya mungkin saling tumpang tindih.

SSL tidak memberi apa-apa kecuali handshake dan enkripsi. Diperlukan aplikasi untuk membuat SSL menjalankan tugasnya. SSH sebaliknya menjalankan menjalankan sendiri banyak hal. Dua hal penting SSH adalah console login (menggantikan telnet) dan secure filetransfer (menggantikan FTP), tetapi dengan SSH anda juga memperoleh kemampuan membentuk source tunnel untuk melewatkan HTTP,FTP,POP3, dan apapun lainnya melalui SSH tunel.

Tanpa adanya traffic dari suatu aplikasi, SSL tidak melakukan apa-apa, tetapi SSH sudah membentuk encrypted tunel antara dua host yang memungkinkan untuk melakukan login shell, file transfer, dan lain sebagainya.

HTTPS menggunakan SSL untuk menjalankan HTTP yang secure dan HTTPS itu dapat dilewatkan melalui tunel yang dibentuk oleh SSH.

Cara Kerja SSH dan SSL

1. Cara Kerja SSH

Misalkan suatu client mencoba mengakses suatu linux server melalui SSH. SH daemon yang berjalan baik pada linux server maupun SSH client telah mempunyai pasangan public/private key yang masing-masing menjadi identitas SSH bagi keduanya. Langkah-langkah koneksinya adalah sebagai berikut :

Langkah 1

Client bind pada local port nomor besar dan melakukan koneksi ke port 22 pada server.

Lankah 2

Client dan server setuju untuk menggunakan sesi SSH tertentu. Hal ini penting karena SSH v.1 dan v.2 tidak kompatibel.

Langkah 3

Client meminta public key dan host key milik server.

Langkah 4

Client dan server menyetujui algoritma enkripsi yang akan dipakai (misalnya TripleDES atau IDEA).

Langkah 5

Client membentuk suatu session key yang didapat dari client dan mengenkripsinya menggunakan public key milik server.

Langkah 6

Server men-decrypt session ky yang didapat dari client, meng-re-encrypt-nya dengan public key milik client, dan mengirimkannya kembali ke client untuk verivikasi.

Langkah 7

Pemakai mengotentikasi dirinya ke server di dalam aliran data terenkripsi dalam session key tersebut.

Sampai disini koneksi telah terbentuk, dan client dapat selanjutnya bekerja secara interaktif pada server atau mentransfer file ke atau dari server. Langkah ketujuh diatas dapat dilaksanakan dengan berbagai cara (username/password, kerberos, RSA dan lain-lain).

2. Cara Kerja SSL

Cara kerja SSL dapat kita lihat dengan tahapan – tahapan :

Langkah 1

Client membentuk koneksi awal ke server dan meminta koneksi SSL.

Langkah 2

Bila server yang dihubungi telah dikonfigurasi dengan benar, maka server ini akan mengirimkan client *public key* miliknya.

Langkah 3

Client membandingkan sertifikat dari server ke basisdata trusted authorities. Bila sertifikat ini terdaftar di situ, artinya client mempercayai (trust) server itu dan akan maju kelangkah 4. Bila sertifikat itu terdaftar, maka pemakai harus menambahkan sertifikat ini ke *trusted database* sebelum maju ke langkah 4.

Langkah 4

Client menggunakan *Public Key* yang didapatnya untuk men-enkrip sesi dan mengirimkan *session key ke server*. Bila server meminta sertifikat client di langkah2, maka clent harus mengirimkannya sekarang.

Langkah5

Bila server di-setup untuk menerima sertifikat, maka server akan membandingkan sertifikat yang diterimanya dengan basisdata *trusted authorities* dan akan menerima atau menolak koneksi yang diminta.

Bila kondisi ditolak, suatu pesan kegagalan akan dikirimkan ke client. Bila koneksi diterima, atau bila server tidak di-setup untuk menerima sertifikat, maka server akan men-decode *session key* yang didapat dari client dengan privete key milik server dan mengirimkan pesan berhasil ke client yang dengan demikian membuka suatu *secure data chanel.*

3. Implementasi SSH dan SSL

Implementasi SSH terlihat dalam produk-produk berikut :

FreeSSH

- OpenSSH (Unix, Windows)
- LSH (unix)
- PuTTY (Windows)
- Okhapkin s port of SSH1(windows)
- MacSSH (Macintosh)
- TeraTerm (windows)
- MindTerm (Inix, Windows)
- NitfyTelnet 1.1 SSH (Machintosh)

Commercial SSH

- SSH communication Security (unix, windows)
- F-Secure SSH (unix,Windows)
- Secure CRT, SecureFX (windows)
- Vshell (Windows)

Implementasi SSL

Terdapat dua implementasi SSL: SSLeay dan OpenSSL. Microsoft menerapkan versi SSH-nya sendiri yang dikenal sebagai TSL atau Transport Layer Security (disebut juga sebagai SSL v.3.1), namun tidak mendapat banyak dukungan diluar produk-produk Microsoft sendiri.

IV. KESIMPULAN

1. SSH maupun SSL digunakan untuk mengamankan komunikasi melalui internet
2. SSH mendukung otentikasi terhadap remote host, sehingga meminimalkan ancaman pemalsuan identitas client lewat IP address spoofing maupun manipulasi DNS.
3. SSH mendukung beberapa protokol enkripsi secret key (DES,TripleDES,IDEA, dan Blowfish) untuk membantu memastikan privacy dari keseluruhan komunikasi, yang dimulai dengan username/password awal
4. SSL mendukung beberapa protokol enkripsi dan memberikan autentikasi client dan server
5. SSL beroperasi pada layer transpor, menciptakan saluran enkripsi yang aman untuk data, dan dapat mengenkripsi banyak tipe data

V. DAFTAR PUSTAKA

NEOTEK Vol III No.04 Januari 2003
http://www.polibatam.ac.id/~webmaster/print.php?sid=73