SISTEM KEAMANAN ENKRIPSI
SECURE SHELL (SSH) UNTUK KEAMANAN DATA

Ika Dwi Cahyani *)

ABSTRAKSI.

Keamanan data pada system computer saat ini merupakan kebutuhan yang urgen, mengingat semakin luas jangkauan internet dalam sisi teknologi dan regional wilayah. 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 protocol enkripsi secret key (DES, TripleDES, IDEA, dan Blowfish) untuk membantu memastikan privacy dari keseluruhan komunikasi,

Keyword: Keamanan data, enkripsi, SSH,

1. **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 bias 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.*

Ia dapat digunakan untuk login secara aman, misalnya ke remote host atau menyalin data antar host, sementara mencegah man-in-the-middle attacks (pembajakan sesi) dan DNS spoofing. Ia akan melakukan kompresi data pada koneksi anda, dan komunikasi X11 yang

---

*) Jur Teknik Elektronika Fak Teknik Universitas Pandanaran

aman antar host.

2. PENGERTIAN SECURE SHELL (SSH).

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 protocol 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-themiddle 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.

3. SECURE SHELL

SSH adalah program yang memungkinkan anda untuk login ke sistem remote dan memiliki koneksi yang terenkripsi. 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.

SSH sangat murah, bahkan gratis untuk penggunaan non-komersial dan biaya sedikit untuk penggunaan komersial. SSH tersedia dua versi SSH-1 dan SSH-2.

SSH-2 adalah versi terbaru dan paling aman dan SSH-1 masih sangat popular (dapat ditemukan sebagai lisensi GPL untuk semua platform). Dan memiliki beberapa keterbatasan dalam fitur dan memiliki beberapa masalah keamanan yang berbahaya, misalnya menggunakan CRC untuk perlindungan integritas tidak aman. SSH memiliki ketersediaan tinggi dan berjalan pada hampir seluruh platform. SSH-2 guna mendukung banyak algoritma enkripsi seperti 3DES, IDEA, Blowfish, Twofish dan Cast. SSH VPN dalam bentuk yang paling sederhana menggunakan kemampuan SSH ke port layanan

terowongan di Internet di dalam sebuah session SSH. Meskipun memiliki keterbatasan, mudah untuk melakukan setup, kebutuhan non-administratif akses dan bekerja dengan andal.
Anda dapat pula menggunakan SSH dari stasiun kerja Windows anda ke server SSH Linux. Terdapat beberapa implementasi client Windows yang tersedia gratis dan juga implementasi komersil dari DataFellows.

- Manfaat .

Manfaat SSH diantaranya untuk terowongan berbasis TCP aplikasi melalui SSH, misalnya email protokol, tool pemrograman dan bahkan aplikasi bisnis seperti Oracle. Untuk sebagian besar pengguna SSH tampaknya terminal emulator mirip dengan Telnet. Para pengguna tidak melihat enkripsi dan oleh karena itu keamanan transparan bagi pengguna. Untuk administrator sistem SSH adalah populer remote administrasi platform.

- Keterbatasan

SSH tidak dirancang untuk dimasukkan ke gateway jaringan seperti router atau firewall sebagai solusi lengkap VPN. Hal ini dimungkinkan untuk membuat VPN dengan tunneling PPP melalui SSH, tetapi membutuhkan banyak overhead dan tidak dimaksudkan untuk menangani koneksi dengan banyak kebutuhan bandwidth seperti IPsec. TLS / SSL dan IPsec hampir benar-benar transparan untuk digunakan, tetapi SSH tidak, untuk menggunakan SSH Anda harus login ke account pengguna untuk memanfaatkan keamanan lapisan transport. SSH digunakan untuk aplikasi scripting, sedangkan TLS / SSL dan IPSec adalah dimasukkan ke dalam aplikasi dan TCP / IP stack. UDP dan ICMP juga masalah dengan SSH. Tidaklah mungkin untuk terowongan lalu lintas UDP atau ICMP. Protokol-protokol ini memang dapat berguna dalam beberapa VPN, misalnya mengamankan audio streaming melalui VPN. Masalah lain dengan SSH adalah bahwa ada begitu banyak implementasi berbeda dari protokol bahwa masalah interoperabilitas adalah mulai muncul, misalnya implementasi yang berbeda dari server mungkin tabrakan dengan klien dan wakil sebaliknya. Hal ini terjadi meskipun yang SSH menjadi standar oleh IETF.

- Dasar-dasar SSH.

Menurut OpenSSH page OpenSSH adalah versi FREE dan SSH sebagai tool untuk melakukan konektivitas pada jaringan. Jika anda menggunakan telnet, rlogin, dan ftp mungkin tanpa anda sadari bahwa password yang terkirim tanpa melalui enkripsi. Sedangkan dengan menggunakan OpenSSH melakukan enkripsi kepada semua trafik (termasuk password), secara efektif untuk menghindari hal-hal

yang tidak diinginkan. Secara tambahan, Open SSH memiliki tunneling yang aman dan beberapa metode autentikasi dan juga mendukung semua versi protokol SSH.

Open SSH sangatlah pas untuk bisa menggantikan rlogin dan telnet dengan program SSH, rcp dengan SCP dan ftp dengan sftp. Juga termasuk sshd (paket server-side), dan juga tool lain seperti ssh-add, ssh-agent, ssh-keysign, sshkeyscan, ssh-keygen dan sftp-server.

Suatu contoh dalam SSH Client, anda asumsikan memiliki account di server : namaserver.com (ip address) dan mesin tersebut menjalankan ssh server. Account Anda pada server di refer pada username dan password Anda misal password 123. Untuk dapat masuk menggunakan ssh, anda dapat dengan melakukan perintah :

ssh -l username : namaserver.com atau jika Anda belum memiliki namaserver, dengan menggunakan ip address :

ssh -l username xxx.xxx.xxx.xxx (x merepresentasikan ip address) alternatif jika tidak menggunakan parameter -l : ssh username@namaserver.com atau ssh username@xxx.xxx.xxx.xxx

Dengan melakukan perintah tersebut Anda lalu akan diminta memasukkan password. SCP Client Selain itu kita juga bisa melakukan copy file. Misal Anda akan melakukan transfer file yang bernama file.txt pada mesin yang berbeda :

scp /home/username/file.txt username@namaserver.com:~/home/username/

Pertama kita menuliskan perintah scp, selanjutnya kita menentukan letak file yang ingin kita copy berada “/home/username/file.txt”. Lalu seperti menggunakan ssh selanjutnya kita menentukan username dan namaserver, terakhir menentukan letak file yang ingin kita tuju “:~/home/username/”.

Jika kita ingin mengcopy isi folder dengan menambahkan parameter -r seperti ini :

scp -r /home/username/direktori username@namaserver.com:~/home/username/

Jika mengubah port dari SSH, standarnya port ssh adalah 22, dengan mengubahnya, maka saat anda melakukan koneksi dari client anda harus menspesifikasikan port tersebut, misal : ssh -l username xxx.xxx.xxx.xxx 44

Pada port tersebut telah di buka. Juga buka file konfigurasi untuk opsi lebih lanjut yang dapat diubah : /etc/ssh/ssh_config (untuk client) dan atau /etc/ssh/sshd_config (untuk server). Jika merubah apapun yang ada di sshd_config, jangan lupa untuk merestart kembali ssh server tersebut.

- Public Key Cryptografi.

SSH menggunakan metode public-key cryptography untuk mengenkripsi komunikasi antara dua host, demikian pula untuk autentikasi pemakai. Dengan metode ini, kita akan memerlukan 2 buah kunci

berbeda yang digunakan baik untuk melakukan enkripsi dan dekripsi. Dua buah kunci tersebut masing-masing disebut public key (dipublikasikan ke publik/orang lain) dan private key (dirahasiakan/hanya pemiliknya yang tahu). Masing-masing kunci di atas dapat digunakan untuk melakukan enkripsi dan dekripsi.

SSH dapat digunakan untuk login secara aman ke remote host atau menyalin data antar host, sementara mencegah man-in-themiddle 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. SSH merupakan produk serbaguna yang dirancang untuk melakukan banyak hal, yang kebanyakan berupa penciptaan tunnel antar host.

4. KEGUNAAN SECURE SHELL

SSH dirancang untuk menggantikan protokol telnet dan FTP yang mempunyai banyak fitur lain, tetapi tujuan utamanya memang untuk mengamankan komunikasi melalui internet. 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 dapat menjalankan sendiri banyak hal, dua hal penting SSH yaitu console login (menggantikan telnet) dan secure filetransfer (menggantikan FTP), juga memperoleh kemampuan membentuk source tunnel untuk melewatkan HTTP, FTP, POP3, dan apapun lainnya melalui SSH tunel.

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

- 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.

Langkah 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 mengenkripsinyamenggunakan 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).

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.*

5. IMPLEMENTASI SSH

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.

6. KESIMPULAN.

1. SSH 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.

DAFTAR PUSTAKA

Budi Rahardjo, *"Keamanan Sistem Informasi Berbasis Internet*", PT Insan Infonesia, 2002

Ivan Sudirman, "*TCP/IP dan Praktek Sekuriti Jaringan", ilmukomputer.com*, 2003

T. Ylonen, "The Secure Shell (SSH) Protocol Architecture", Copyright (C) The Internet Society, 2006

http://www.ristishop.com/index.php?ch=8&lang=ind&s=4d6b2b805828f1c8b529348ac 00fdb51&n=308, 28 Desember 2008, 13.32

http://searchsecurity.techtarget.com/sDefinition/ 0,,sid14_gci212845,00.html, 28 Desember 2008, 13.32

http://searchsecurity.techtarget.com/sDefinition/ 0,,sid14_gci214091,00.html, 28 Desember 2008, 13.33