Perbandingan metode pengamanan data pada SSL (Secure Socket Layer) dan SSH (Secure Shell)

Triadi Wirawan (23213370)

INTISARI

Kejahatan pada dunia internet sudah sangat marak terjadi sekarang. Dengan perkembangan teknologi informasi pesat, membuat kesempatan berbuat jahat dengan memanfaatkan internet juga semakin meningkat. Keamanan dalam penyimpanan data menjadi sangat vital dalam dunia internet. Oleh karenanya perlu ada pengamanan dalam hal ini. Banyak metode yang digunakan untuk mengamankan data. Pada makalah ini penulis mencoba mengkaji dua metode enkripsi data pada SSL (Socket Secure Layer) dan SSH (Secure Shell). SSL 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. 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. 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.

Kata Kunci : *SSH, SSL, Enkripsi, Keamanan data*

ABSTRACT

Crime on the Internet world has been very rampant now. With the rapid development of information technology, making the opportunity to do crime by utilizing the Internet have also increased. Security in data storage is vital in the world of internet. Therefore there needs to be safeguards in this regard. Many methods are used to secure data. In this paper, the authors try to examine two methods of data encryption on the SSL (Secure Socket Layer) and SSH (Secure Shell).

SSL supports several encryption protocol and provide authentication of client and server. SSL operates at the transport layer, creates a secure encrypted channel for data, and can encrypt data of many types.

SSH is a suite of programs used as a secure replacement for rlogin, rsh and rcp. It uses public-key cryptography to encrypt communications between two hosts, as well as to authenticate users.

SSL is designed to secure web session, while SSH is designed to replace telnet and FTP protocols. Both have many other features, but its main purpose was to secure communications over the internet.

Keywords : *SSH, SSL, encription, data security*

BAB 1 : Pendahuluan

1 . 1 . Latar Belakang

Pengiriman data dalam suatu jaringan komputer tidak terlepas dari berbagai permasalahan yang bisa saja terjadi. Ini karena, sebelum data yang kita kirim sampai ke tempat tujuan maka akan melewati serangkaian proses terlebih dahulu. Data yang sedang dalam proses pentransmisian data pada suatu jaringan pada dasarnya memiliki tingkat keamanan yang rendah. Jadi data tersebut sangat rentan dibobol atau disusupi oleh pihak lain.

Tindakan pembobolan (hacking) itu sangat merugikan bagi kita, apalagi jika data yang dikirim merupakan data penting atau data yang sangat rahasia. Mereka bisa saja memanfaatkan data kita untuk melakukan tindakan yang tidak bertanggung jawab tanpa memikirkan hal tersebut bisa saja merugikan orang lain, bahkan diri kita sendiri.

Seiring dengan berbagai tindak kejahatan yang terjadi dengan memanfaatkan kelemahan pada suatu jaringan. Juga berkembang beberapa teknik pengamanan yang bisa digunakan untuk meminimalisir resiko terjadinya kejahatan tersebut. Seperti yang dijelaskan dalam suatu penelitian, bahwa tidak ada suatu jaringan yang benar-benar aman, teknologi yang ada dibuat hanya untuk mengurangi resiko kejahatan yang bisa saja terjadi.

Jadi, dengan meningkatkan sistem keamanan data pada jaringan komputer, kita dapat berupaya mempersulit para hacker atau cracker di saat mencoba membobol atau merusak sistem jaringan kita, sehingga mereka tidak bisa dengan mudahnya melakukan tindakan yang dapat merugikan.

1 . 2 . Maksud & Tujuan

Makalah ini bertujuan untuk mengetahui perbedaan dan manfaat dari metode pengamanan data SSL & SSH, dengan maksud pembaca dapat memahami penggunaan dari masing-masing metode tersebut dan memanfaatkannya dalam kegiatan berselancar di dunia maya.

1 . 3 . Metode Penulisan

Dalam makalah ini metode penulisan yang digunakan adalah studi literatur dimana sumber berasal dari artikel dan jurnal yang ada di internet.

BAB 2 : Secure Socket Layer (SSL)

2 . 1 . Pengertian SSL

SSL adalah protokol keamanan yang digunakan pada hampir semua transaksi aman pada internet. SSL mengubah suatu protokol transport seperti TCP menjadi sebuah saluran komunikasi aman yang cocok untuk transaksi yang sensitif seperti Paypal, Internet Banking, dan lain-lain. Keamanan dijamin dengan menggunakan kombinasi dari kiptografi kunci publik dan kriptografi kunci simetri bersamaan dengan sebuah infrastruktur sertifikat. Sebuah sertifikat adalah sebuah kumpulan data identifikasi dalam format yang telah distandardisasi. Data tersebut digunakan dalam proses verifikasi identitas dari sebuah entitas (contohnya sebuah web server) pada internet.

SSL menyediakan otentikasi (pada sisi client, dan opsional pada sisi server) terhadap pihak-pihak yang berkomunikasi. SSL dapat mengamankan koneksi antara dua titik, dan tidak ada pihak yang dapat melakukan hal-hal yang bersifat destruktif atau mengakses informasi yang bersifat sensitif. SSL menyediakan sebuah saluran komunikasi yang aman tanpa perlu adanya pertemuan kedua pihak yang berkomunikasi untuk melakukan proses pertukaran kunci.

Implementasi SSL paling pertama dikembangkan oleh Netscape Communications Corporation pada awal tahun 1990-an untuk mengamankan HTTP. Pada akhir tahun 1990-an, semakin terlihat dengan jelas bahwa SSL 2.0 tidaklah aman. Netscape memulai untuk membangun SSL 3.0. Dengan bantuan Netscape, Internet Engineering Task Force (IETF, badan yang mengatur untuk standar internet) memulai untuk menstandardisasi SSL, sebuah proyek yang kemudian dikenal dengan nama TLS (Transport Layer Security). SSL 3.0 tidak dikembangkan seteliti TLS, sehingga SSL 3.0 dapat dirilis lebih dahulu dan

menggantikan SSL 2.0 sebagai standar industri. TLS yang akhirnya diselesaikan pada tahun 2000, menyediakan protokol terstandardisasi yang pertama untuk SSL. Walaupun SSL 3.0 masih digunakan secara luas, untuk pengembangan terbaru termasuk sudah tertinggal karena saat ini hampir semua browsermodern mendukung TLS.

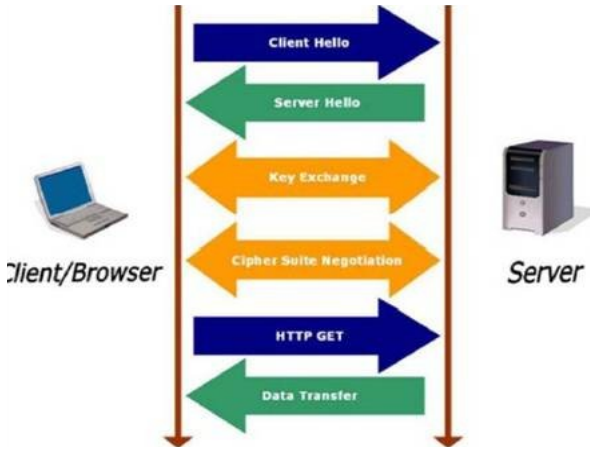
2 . 2 . Fungsi SSL

Fungsi SSL pada komunikasi aman sama seperti fungsi TCP pada komunikasi normal, yaitu menyediakan sebuah infrastruktur komunikasi standar di mana sebuah aplikasi dapat menggunakannya dengan mudah dan hampir tidak dapat terlihat (invisible). SSL menyediakan sebuah komponen penting pada sistem yang aman.

Mekanisme otentikasi dasar seperti password Telnet dan otentikasi HTTP dasar menjadi sangat kuat ketika dieksekusi dengan SSL dibandingkan dengan TCP, di mana pada SSL password tidak lagi dikirim dalam bentuk plainteks. SSL mengenkripsi koneksi, bukan data pada kedua pihak yang berkomunikasi, dan tidak mengandung mekanisme untuk otentikasi user ataupun perlindungan password (hanya koneksi yang diotentikasi, keamanannya akan gagal jika mesin pada kedua pihak yang berkomunikasi compromised).

2 . 3 . Cara Kerja SSL

Secara umum, cara kerja protokol SSL adalah sebagai berikut (lihat Gambar 1) :



1. Klien membuka suatu halaman yang mendukung protokol SSL, biasanya diawali dengan “https://” pada browsernya.
2. Kemudian webserver mengirimkan kunci publiknya beserta dengan sertifikat server.
3. Browser melakukan pemeriksaan : apakah sertifikat tersebut dikeluarkan oleh CA (Certificate Authority) yang terpercaya? Apakah sertifikat tersebut masih valid dan memang berhubungan dengan alamat situs yang sedang dikunjungi?
4. Setelah diyakini kebenaran dari webserver tersebut, kemudian browser menggunakan kunci public dari webserver untuk melakukan enkripsi terhadap suatu kunci simetri yang dibangkitkan secara random dari pihak klien. Kunci yang dienkripsi ini kemudian dikirimkan ke webserver untuk digunakan sebagai kunci untuk mengenkripsi alamat URL (Uniform Resource Locator) dan data http lain yang diperlukan.
5. Webserver melakukan dekripsi terhadap enkrispi dari klien tadi, menggunakan kunci privat server. Server kemudian menggunakan kunci simetri dari klien tersebut untuk mendekripsi URL dan data http yang akan diperlukan klien.
6. Server mengirimkan kembali halaman dokumen HTML yang diminta klien dan data http yang terenkripsi dengan kunci simetri tadi.
7. Browser melakukan dekripsi data http dan dokumen HTML menggunakan kunci simteri tadi dan menampilkan informasi yang diminta.

BAB 3 : Secure Shell (SSH)

3 . 1 . Pengertian SSH

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 untuk membantu memastikan privacy dari keseluruhan komunikasi, yang dimulai dengan username/password awal.

SSH pertama kali dikembangkan oleh Tatu Yl nen di Helsinki University of Technology. Beliau adalah orang pertama yang mendesain suatu protocol network yang secure. Karena sering terjadi password-sniffing pada network di universitas tersebut. Beliau membuat SSH1 dengan teknik enkripsi.

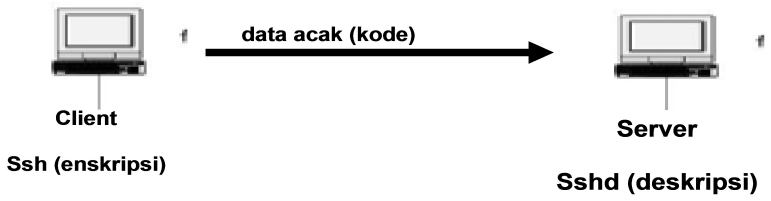
Algoritma enkripsi yang didukung oleh SSH di antaranya TripleDES(Pengembangan dari DES oleh IBM), BlowFish (BRUCE SCHNEIER), IDEA (The International Data Encryption Algorithm), dan RSA (The Rivest-Shamir-Adelman). Dengan berbagai metode enkripsi yang didukung oleh SSH, Algoritma yang digunakan dapat diganti secara cepat jika salah satu algoritma yang diterapkan mengalami gangguan. SSH 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.

3 . 2 . Fungsi SSH

SSH dirancang untuk menggantikan protokol telnet dan FTP. SSH merupakan produk serbaguna yang dirancang untuk melakukan banyak hal, yang kebanyakan berupa penciptaan tunnel antar host. 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.

3 . 3 . Cara Kerja SSH

Saat 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 :

1. Client bind pada local port nomor besar dan melakukan koneksi ke port 22 pada server.
2. Client dan server setuju untuk menggunakan sesi SSH tertentu. Hal ini penting karena SSH v.1 dan v.2 tidak kompatibel.
3. Client meminta public key dan host key milik server.
4. Client dan server menyetujui algoritma enkripsi yang akan dipakai (misalnya TripleDES atau IDEA).
5. Client membentuk suatu session key yang didapat dari client dan mengenkripsinya menggunakan public key milik server.
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 verifikasi.
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).

BAB 4 : 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.

Daftar Pustaka

[1] http://www.te.ugm.ac.id/~risanuri/distributed/TELNET.pdf

[2] https://icalgom.wordpress.com/2012/10/07/ssh-sftp-dan-scp/

[3] http://iskandar-zulkarnaen1.tripod.com/ssh.pdf

[4] https://icalgom.files.wordpress.com/2012/10/2.jpg

[5] https://31.media.tumblr.com/

[6] http://www.scribd.com/doc/14682116/Belajar-Ssh?autodown=pdf