IMPLEMENTASI SECURE MAIL MENGGUNAKAN ENKRIPSI PADA GNUPG

TUGAS AKHIR

Diajukan sebagai salah satu syarat untuk mendapatkan gelar Ahli Madya
Pada Jurusan Tekonologi Informasi Program Studi Teknik Komputer

Oleh :

RIGORISTO
BP.06093018

PROGRAM STUDI TEKNIK KOMPUTER
JURUSAN TEKNOLOGI INFORMASI
POLITEKNIK UNIVERSITAS ANDALAS
PADANG
2009

ABSTRAKSI

Perangkat lunak dalam jaringan komputer semakin berkembang. Baik pada skala LAN, MAN,WAN dan Internet. Keamanan data akan menjadi masalah utama dalam menghadapi perkembangan teknologi. Pengamanan informasi tidak hanya sebatas mengupayakan agar informasi tersebut tidak dibaca oleh pihak yang tidak berkepentingan, tetapi juga bagaimana agar informasi tersebut tidak dapat dimanipulasi atau dimodifikasi. Salah satu cara mengatasi hal ini adalah dengan mengenkripsi email. *GNU Privacy Guard* adalah sistem enkripsi *key public*. Setiap pengguna yang memanfaatkan layanan email akan merasa aman akan informasi yang telah dikirim maupun diterima karena telah memnfaatkan layanan enkripsi email.

GnuPG dapat dimanfaatkan oleh seluruh pengguna email untuk menjaga keamanan informasi dari pihak-pihak yang tidak berkepentingan. GnuPG berlisensi gratis, juga memiliki banyak fitur keamanan termasuk tandatangan digital.

Kata kunci : Jaringan Internet, GnuPG (*Gnu Privacy Guard*) windows, Kgpg, Thunderbird dan Kmail.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Email sudah digunakan orang sejak awal terbentuknya internet pada sekitar tahun 1969 dan merupakan salah satu fasilitas yang ada pada saat itu. Sesuai dengan perkembangan internet, penggunaan email ini juga semakin membesar walaupun pada saat ini persentasinya sudah turun karena adanya sebuah fasilitas baru di internet yang dikenal sebagai Web. Salah satu alasan kenapa email dipakai orang karena memberikan cara yang mudah dan cepat dalam mengirimkan sebuah informasi. Selain itu dengan email dapat juga informasi yang ukurannya kecil sampai ke *file* yang ukurannya besar.

Sangat pentingnya nilai sebuah informasi menyebabkan seringkali informasi diinginkan hanya boleh diakses oleh orang-orang tertentu. Jatuhnya informasi ke tangan pihak lain (misalnya pihak lawan bisnis) dapat menimbulkan kerugian bagi pemilik informasi. Keamanan dari layanan email yang digunakan harus terjamin dalam batas yang dapat diterima.

Namun sifat email yang memanfaatkan penghantar elektronik tak sepenuhnya dimaksudkan sebagai medium pribadi karena menyimpan potensi bahaya penyalahgunaan yang bukan saja menjengkelkan tetapi juga dapat bersifat fatal.

Saat ini banyak email palsu yang menggunakan identitas seseorang, baik yang dihasilkan oleh program seperti *worm* ataupun sengaja dilakukan oleh pihak tertentu

yang tidak bertanggung jawab. Dalam kondisi seperti ini penggunaan teknik otentifikasi pesan sangat diperlukan untuk memastikan bahwa email yang diterima dari pengirim valid. Server email menerima pesan dan mengirimkannya ke alamat yang dituju seperti pengiriman surat yang tinggal dimasukkan ke kotak surat dan akan dikirimkan ke alamat yang dituju oleh tukang pos. Otentifikasi terhadap email pada umumnya hanya dilakukan terhadap alamat *IP* komputer pengirim, dan sepanjang alamat tersebut dianggap valid, maka siapapun dapat menulis email dari komputer tersebut.

Ketika kita mengirimkan suatu email, maka email tersebut disampaikan ke suatu sistem komputer yang mungkin kita tidak mengetahui administratornya. Dari komputer tersebut disampaikan ke sistem komputer lain, dan yang lainnya, dan lainnya, sampai kepada penerima yang dituju. Pada beberapa link di rantai ini, email kita dapat dibaca oleh siapa saja yang diinginkan *system administrator* atau oleh suatu biro penyelidikan yang sedang mencurigai suatu aktivitas kejahatan, atau berbagai kemungkinan lainnya. Tetapi secara ringkasnya adalah ketika kita mengirimkan suatu email, kita tidak mengetahui siapa yang membaca pesan itu, penerima yang diharapkan ataupun barangkali orang lain.

Kerahasiaan email terancam bukan oleh para *hacker*, melainkan para *system administrator* sendiri. Para *system administrator* terkadang bosan tidak tahu apa yang harus dikerjakan selain membaca-baca email orang. Mereka dapat melakukannya tanpa sedikit pun meninggalkan jejak.

BAB V

KESIMPULAN

5.1 Kesimpulan

Kesimpulan yang dapat diambil dari pembuatan tugas akhir ini adalah :

1) GnuPG merupakan software enkripsi yang bersifat *open source* dan kompetibel dengan sistem operasi windows dan linux.

2) Ketersediaan beberapa algoritma di dalam *software* GnuPG juga membuat pengguna bisa lebih leluasa untuk mengatur kerahasiaan pesannya.

3) Tanda tangan digital merupakan salah satu penggunaan metode kriptografi yang bertujuan untuk mendeteksi modifikasi data yang tidak sah (*unauthorized modification of data*) dan untuk mengecek otentikasi identitas dari pengirim dan *non repudiation* (menolak penyangkalan)

5.2 Saran

Berdasarkan hasil yang telah diperoleh selama proses implementasi, ada beberapa saran yang perlu disampaikan demi menjaga keamanan email yaitu:

1) Masalah keamanan pengiriman email/dokumen harus selalu sosialisasikan kepada masyarakat, khususnya pengguna internet.

2) Pengguna sebaiknya selalu waspada terhadap kemungkinan adanya *bug* (kelemahan) pada setiap perangkat lunak, termasuk GnuPG. Dan jika menemukan *bug* tersebut, sebaiknya segera dipublikasikan terutama ke pihak pengembang.

DAFTAR PUSTAKA

Sopandi, Dede. "Pengantar Komunikasi Data". Bandung : Informatika, 2005

Tanenbaum, Andrew.S. "Jaringan Komputer.Prenhallindo". Jakarta, 1997

Mulyana, Y.B. "Linux Semudah Windows". Elex Media Komputindo : Jakarta, 2002

Koch, Werner."Using The GNU Privacy Guard", The Free Software Foundation, 2007

Munir, Rinaldi." Diktat Kuliah IF5054 Kriptografi". STEI ITB, 2007

Stallings, William. "Cryptography and Network Security".*Third Edition*. Prentice hall. USA, 2003