PENERAPAN SISTEM KEAMANAN *ELECTRONIC MAIL* (E-MAIL) BERBASIS *Gnu PRIVACY GUARD* (GnuPG)

SKRIPSI

Diajukan untuk Menempuh Ujian Akhir sarjana
Fakultas Teknik
Program Strata I Jurusan Teknik Informatika
Universitas Komputer Indonesia

SEPTI KURNIAWATI JUMI'AH
10199061

PROGRAM STRATA I
JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS KOMPUTER INDONEISA
BANDUNG
2003

KATA PENGANTAR

Bismillahirahmaanirrahim

Puji dan syukur atas segala karunia dan pertolongan-Nya yang tiada terhingga sehingga penulis dapat menyelesaikan skripsi yang berjudul " Penerapan Sistem Keamanan *Elektronik Mail* (e-mail) berbasis *Gnu Privacy Guard* (GnuPG) ". Skripsi ini disusun untuk memenuhi persyaratan menempuh ujian Sarjana jurusan Teknik Infomatika Universitas Komputer Indonesia, Bandung.

Meskipun demikian penulis menyadari bahwa skripsi ini masih memiliki banyak kekurangan dan kelemahan. Penulis menerima saran dan kritik yang membangun dari pembaca agar dapat digunakan sebagai bahan kajian untuk menulis karya ilmiah yang lebih baik. Penulis berharap agar suatu saat tulisan ini bisa disempurnakan.

Skripsi ini terwujud berkat bantuan dan dukungan dari berbagai pihak. Untuk itu penulis mengucapkan terima kasih sedalam-dalamnya kepada :

1. Bapak, Ibu dan kedua adikku yang telah memberikan dukungan secara moril, material, dan spiritual.
2. Bapak Ir. Eddy Suryanto Soegoto, M.Sc, selaku Rektor Universitas komputer Indonesia.
3. Bapak Prof. Dr. Ir. Prayoto, M.Sc, selaku Dekan Fakultas Teknik Universitas Komputer Indonesia.

4. Bapak Budhi Irawan, S.Si, selaku Ketua Jurusan teknik Informatika Universitas Komputer Indonesia.
5. Bapak Muhammad Yusan, MT, selaku Dosen Pembimbing I, yang telah memberikan arahan, bimbingan ,dan pengetahuan yang berguna dalam pengerjaan skripsi ini.
6. Bapak Muhammad Nasrun S.Si, selaku selaku Dosen Pembimbing II, yang telah memberikan arahan, bimbingan ,dan pengetahuan yang berguna dalam pengerjaan skripsi ini.
7. Seluruh staf dosen dan karyawan jurusan Teknik Informatika UNIKOM serta pihak-pihak lain yang tidak dapat penulis sebutkan namanya satu persatu.

Semoga Allah SWT membalas dengan yang lebih baik. Suatu pengharapan besar semoga tulisan ini bermanfaat dan membuka wawasan kita untuk selalu bisa berinovasi terhadap suatu hal yang baru. Mudah-mudahan Allah SWT memasukkan kita pada golongan orang-orang yang sabar, bersyukur, mencintai ilmu dan berilmu pengetahuan.

Bandung, Agustus 2003

Penyusun

DAFTAR ISI

LEMBAR PENGESAHAN

KATA PENGANTAR i

DAFTAR ISI iv

DAFTAR GAMBAR vi

ABSTRAKSI viii

ABSTRACT ix

BAB I PENDAHULUAN

1.1 Latar Belakang 1

1.2 Identifikasi Masalah 2

1.3 Batasan Masalah 3

1.4 Maksud dan Tujuan 3

1.5 Metodologi Penelitian 4

1.6 Sistematika Penulisan 5

BAB II LANDASAN TEORI

2.1 Konsep Jaringan Komputer 8

2.1.1 Tipe Jaringan Komputer 10

2.1.2 Arsitektur Jaringan Komputer 13

2.1.3 Media Implementasi Jaringan 15

2.1.4 Perangkat Keras pada LAN 17

2.2 Konsep TCP/IP 21

2.2.1 Dasar Arsitektur TCP/IP 21

2.2.2 Lapisan-lapisan pada TCP/IP 22

2.3 Konsep e-mail 25

2.4 *Simple Mail Transfer Protocol* (SMTP) 26

2.5 Konsep Keamanan Komputer 28

2.5.1 Aspek Keamanan Komputer 28

2.5.2 Serangan Keamanan Komputer 30

2.6 Konsep Kriptografi 33

2.6.1 Mekanisme Kriptografi 33

2.6.2 Kunci dalam kriptografi 37

2.6.3 Kriptografi Simetrik dan Asimetrik 38

2.6.4 Keamanan Sistem Kriptografi 44

BAB III PENERAPAN GnuPG DALAM SISITEM KEAMANAN ELEKTRONIK MAIL

3.1 Tempat dan Waktu Penelitian 47

3.2 Alat – alat yang digunakan 47

3.3 Langkah – langkah Penelitian 48

3.4 Linux Gnu Privacy Guard (GnuPG) 50

BAB IV ANALISIS DATA HASIL PENELITIAN

4.1 Data Hasil Penelitian..... 72

4.2 Komponen e-mail..... 73

4.3 Pengiriman E-mail Secara Konvensional..... 75

4.4 Pengiriman E-mail Dengan GnuPG..... 77

4.5 Proses Enkripsi dalam Pengiriman e—mail..... 80

4.6 Proses Dekripsi dalam Penerimaan e-mail..... 83

BAB V KESIMPULAN DAN SARAN

5.1 Kesimpulan..... 93

5.2 Saran..... 94

Daftar Pustaka

DAFTAR GAMBAR

Gambar 2.1 Topologi *Bus* 10

Gambar 2.2 Topologi *Ring* 11

Gambar 2.3 Topologi *Star* 12

Gambar 2.4 Kartu Jaringan 19

Gambar 2.5 *Hub*/Konsentrator 19

Gambar 2.6 *Repeater* 20

Gambar 2.7 *Routers* 20

Gambar 2.8 Lapisan TCP/IP 23

Gambar 2.9 Pergerakan Data dalam TCP/IP 24

Gambar 2.10 Pertukaran *e-mail* dalam TCP/IP 25

Gambar 2.11 Mekanisme Kripografi 35

Gambar 2.12 Kriptografi Berbasis kunci 36

Gambar 2.13 Mekanisme Kriptografi Simetrik 40

Gambar 2.14 Mekanisme Kriptografi Asimetrik 42

Gambar 3.1 Diagram Alir Penelitian 48

Gambar 4.1 Pengiriman *e-mail* Konvensional 76

Gambar 4.2 Pengiriman *e-mail* Konvensional pada host 1 76

Gambar 4.3 Penerimaan *e-mail* Konvensional pada host 2 77

Gambar 4.4 Pengiriman *e-mail* dengan GnuPG 78

Gambar 4.5 Pengiriman *e-mail* dengan GnuPG pada host 1 78

Gambar 4.6 *e-mail* yang terenkripsi dengan GnuPG..... 79

Gambar 4.7 Penerimaan *e-mail* dengan GnuPG pada host 2 79

Gambar 4.8 Pengisian *e-mail* host 1 80

Gambar 4.9 Perintah Memasukkan *Public Key* Penerima 81

Gambar 4.10 Teks *e-mail* setelah terenkripsi..... 82

Gambar 4.11 *e-mail* terenkripsi pada host 2..... 83

Gambar 4.12 Memasukkan *Passphrase* pada host 2..... 84

Gambar 4.13 Hasil Enkripsi pada host 2 85

Gambar 4.14 Pengiriman *Attachment File* pada host 1 86

Gambar 4.15 Memasukkan *Public Key*..... 87

Gambar 4.16 *Attachment File* yang terenkripsi pada host 1..... 88

Gambar 4.17 Memasukkan *Passphrase* pada *attachment File*..... 89

Gambar 4.18 Hasil dekripsi pada host 2..... 90

Gambar 4.19 Hasil dekripsi *Attachment File* pada host 2 91

ABSTAKSI

Internet merupakan salah satu sarana komunikasi yang sedang berkembang sekarang. Fasilitas yang disediakan sangat beragam dan menjanjikan kecepatan pengiriman data ataupun informasi. Salah satu layanan aplikasi di Internet yang paling banyak digunakan adalah *Electronic Mail* (e-mail).

Keamanan sistem informasi berbasis Internet menjadi salah satu keharusan untuk diperhatikan. Hal tersebut dikarenakan jaringan Internet yang sifatnya publik dan global pada dasarnya tidak aman. Pada saat data terkirim dari suatu komputer ke komputer lain di dalam Internet, data itu akan melewati sejumlah komputer yang lain yang berarti akan memberikan kesempatan pada user lain untuk menyadap atau mengubah data tersebut.

Usaha-usaha penyadapan proses penyampaian *e-mail* melalui Internet semakin hari semakin meluas. Terlebih setelah masuknya transaksi dunia bisnis ke dunia Internet yang semakin memerlukan tingkat kerahasiaan tertentu

Jika kita merasa data yang ada di sistem adalah hal penting dan memerlukan pengamanan, ada baiknya GnuPG *(Gnu Privacy Guard)* digunakan untuk memperkuat sistem pengamanan data yang ada. Program ini dapat digunakan untuk menyandikan pesan *e-mail*, data atau dokumen rahasia. Program ini dapat juga digunakan untuk mengirimkan data tersandi via jaringan secara aman.

ABSTRACT

Internet represent one of the medium communications which expanding now. Provided facility very immeasurable and promise speed of delivery of data or information. One of the application service on Internet which at most used is called Electronic Mail (e-mail).

Security information system base on Internet become one of compulsion to be paid attention. The mentioned because of Internet which public in character global and basically is not peaceful. At the time of data sent from an computer to other computer in Internet, that data will pass a number of other computer which mean will give opportunity at other user to tap or alter the data.

Tapping efforts processes forwarding the e-mail via Internet progressively day extended. Particularly after entry of business world transaction to world of Internet which progressively need certain secret level.

If us feel data exist in system is important matter and need security, it is better GnuPG (Gnu Privacy Guard) used to strengthen system security of existing data. This program can be used to encode message of e-mail, secret document or data. This program earn is also used to deliver data encoded safely via network .