

KEAMANAN E-MAIL MENGGUNAKAN METODE ENKRIPSI GNUPG DENGAN SQUIRELMAIL DAN THUNDERBIRD

Ewi Ismaredah^{1*}

^{1*} Jurusan Teknik Elektro, Universitas Islam Negeri Riau

Email : Ewi.ismaredah@uin-suska.ac.id, ewi22@yahoo.co.id

ABSTRAK

Saat ini banyak orang yang sudah menggunakan email sebagai media komunikasi, dan Email bukan sekedar pengganti surat menyurat konvensional saja, namun banyak sekali manfaat yang dihasilkannya. *Electronic Mail* atau populer disebut email adalah perangkat lunak system korespondensi antara satu komputer dengan komputer lain dengan menggunakan system jaringan komputer atau internet. Anda dapat mengirim pesan teks, memo, dan laporan ke satu atau banyak orang hanya dalam waktu dua atau tiga menit. Saat berkomunikasi atau berbagi informasi melalui email, tidak jarang kita menyertakan data-data seperti email, username, password atau informasi sensitif lainnya. Untuk melindungi isi email yang sifatnya rahasia tersebut, maka dapat menggunakan fitur **PGP**. PGP digunakan untuk mengenkripsi body isi pesan email. Dengan menggunakan metode ini maka proses pertukaran informasi membutuhkan persetujuan sebelumnya antara pihak pengirim dan pihak penerima dengan melakukan pertukaran "*public key*" sehingga isi pesan jauh lebih terjamin kerahasiaannya.

1.PENDAHULUAN

Di Era Globalisasi saat ini banyak orang yang menggunakan e-mail untuk berkomunikasi, setiap orang memiliki minimal satu akun email atau bahkan beberapa akun di beberapa fasilitas penyedia email. Email bukan sekedar pengganti surat menyurat konvensional, namun banyak sekali manfaat yang dihasilkannya. *Electronic Mail* atau populer disebut email adalah perangkat lunak sistem korespondensi antara satu komputer dengan komputer lain dengan menggunakan system jaringan komputer atau internet. Anda dapat mengirim pesan teks, memo, dan laporan ke satu atau banyak orang hanyadalam waktu dua atau tiga menit.

Setelah anda menerima surat, anda dapat membaca, mencetak, bahkan menghapus surat tersebut dari system anda. Di era modern dan serba teknologi seperti sekarang ini, keberadaan email adalah suatu hal yang sangat penting. Hampir seluruh kegiatan, seperti pertemuan, diskusi, menyebar surat undangan dapat dilakukan di mana saja dan kapan saja dalam satu waktu dan virtual, yaitu dengan memanfaatkan jaringan internet. Email sangat mendukung proses-proses komunikasi, kolaborasi, dan koordinasi secara elektronik dalam satu waktu. Sangat efisien dan menghemat waktu sehingga tidak ada alasan untuk menunda pembicaraan suatu masalah karena masalah-masalah teknis, seperti sulit mengumpulkan orang-orang karena lokasi tempat tinggal menyebar (kendala geografis), jalanan macet, tiket pesawat mahal, undangan yang terlambat datang dan alasan-alasan lainnya.

Penggunaan email sebagai komunikasi formal secara individual ataupun secara kelompok terbukti secara efektif dapat memangkas biaya-biaya seperti biaya transportasi, sewa ruangan,

konsumsi dan ongkos penginapan (untuk kegiatan rapat). Keamanan email harus direncanakan dan dikoordinasikan dengan baik agar dapat melindungi sumber daya (*resource*) dan investasi di dalamnya. Informasi (data) dan service (pelayanan) sudah menjadi sebuah komoditi yang sangat penting. Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi suatu organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan, maupun individual (pribadi). Untuk menjaga keamanan komunikasi ataupun data, pengguna bias menggunakan/melakukan enkripsi, tandatangan digital, ataupun otentifikasi data. Salah satu perangkat lunak yang memanfaatkan kriptografi adalah GNU Privacy Guard (biasa disingkat menjadi GnuPG atau GPG).

GNU PRIVACY GUARD

GnuPG merupakan perangkat lunak open source yang mengimplementasikan standar Open PGP secara lengkap sebagaimana yang didefinisikan pada RFC4880 dan RFC2440. Sebagai perangkat lunak open source, GnuPG merupakan alternative dari perangkat lunak PGP (Pretty Good Privacy). GnuPG biasanya sudah tercakup di dalam kebanyakan distro Linux, seperti Debian, MandrakeSoft, RedHat, dan SuSE. Dengan GnuPG, pengguna bias mengenkripsi dan menandatangani data dan komunikasi. GnuPG merupakan perangkat lunak command line yang mudah diintegrasikan dengan aplikasi lainnya. Meskipun demikian, tersedia juga aplikasi tampilan (frontend) dan pustaka yang mendukungnya.

Meskipun GnuPG kebanyakan digunakan di lingkungan system operasi yang open source seperti Linux dan FreeBSD, kode program GnuPG juga bias digunakan di lingkungan Windows. Open PGP ini merupakan bundel program yang dikemas untuk Linux yang mencakup GnuPG, mutt, mozilla Thunderbird, dan Squirrelmail. Pada makalah ini, penulis melakukan eksperimen dengan menggunakan GnuPG versi Linux.

PENGUNAAN GNU PRIVACY GUARD

Sebagaimana yang telah ditetapkan dalam standar OpenPGP, GnuPG menyediakan layanan integritas pesan dan file data dengan teknologi tandatangan digital, enkripsi, kompresi, dan konversi Radix-64. GnuPG juga menyediakan layanan manajemen dan sertifikat kunci. Untuk menjamin kerahasiaan pesan atau file data, GnuPG menggunakan kombinasi kriptografi kunci simetrik dan kriptografi kunci-publik. Adapun langkah-langkah menjaga kerahasiaan data pada pengiriman suatu pesan dengan melakukan enkripsi pada GnuPG adalah sebagai berikut:

1. Pengirim membuat pesan.
2. Pengirim membangkitkan sebuah bilangan acak atau memberikan sandi lewat (*passphrase*) sebagai *session key* untuk pesan saat ini.
3. Pengirim mengenkripsi *session key* tersebut dengan kunci public masing-masing penerima. Hasil enkripsi *session key* ini menjadi awal dari pesan yang dikirim.
4. Pengirim mengenkripsi pesan (yang biasanya sudah dikompresi) yang akan dikirim dengan menggunakan *session key*.
5. Penerima mendekripsi pesan dengan kunci privatnya.
6. Penerima mendekripsi pesan dengan *session key*. Jika pesan yang diterima merupakan hasil kompresan, maka pesan harus didekompresi.

ALGORITMA DAN FITUR PADA GNU PRIVACY GUARD

GnuPG yang digunakan untuk eksperimen oleh penulis ini menawarkan beberapa macam fitur dan algoritma.

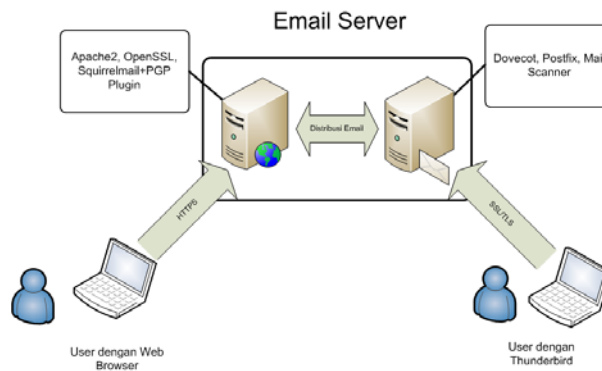
- Berlisensi GPL.
- Implementasi penuh OpenPGP (RFC 2440)

- Mampu menerjemahkan/memverifikasi pesan tersandi dari PGP 5.x
- Mendukung algoritma ElGamal (tanda tangan dan penyandian), DSA, 3DES, BlowFish, TwoFish, CAST5, MD5, SHA-1, RIPE-MD-160 dan TIGER
- Kemudahan implementasi algoritma penyandian baru dengan menggunakan modul ekstensi (*extension module*)
- Identitas pengguna (UserID) diseragamkan dalam suatu bentuk standar.
- Mendukung kunci dan tanda tangan yang dapat kadaluwarsa (hanya dapat digunakan dalam jangka waktu tertentu)
- Dukungan integral untuk HKP Keyserver (www.keys.pgp.net)

2. METODE PENELITIAN

2.1 Perancangan Sistem

Perancangan ini meliputi perancangan perangkat keras dan perangkat lunak seperti pada gambar 1.



Gambar 1. Arsitektur Sistem

2.2 Instalasi Web Server

Berikut ini adalah langkah-langkah instalasi Web Server:

- Untuk mengunduh dan install Web Server Apache beserta library yang dibutuhkan ketik `sudo apt-get install apache2 php5 php5-xmlrpc php5-mysql php5-gd php5-cli php5-curl mysql-client mysql-server`

2.2.1 Instalasi OpenSSL dan SSL Certificate

Instalasi OpenSSL dan SSL Sertifikat ini dilakukan untuk menyediakan layanan keamanan pada koneksi web (https). Langkahnya sebagai berikut

- install OpenSSL dan SSL-Certificate
`# apt-get install openssl ssl-cert`
- Membuat certificate :
`# mkdir /etc/apache2/ssl`
`# make-ssl-cert /usr/share/ssl-cert/ssleay.cnf /etc/apache2/ssl/apache.pem`
- Aktifkan modul SSL dan restart Apache2
`# a2enmod ssl`
`# /etc/init.d/apache2 force-reload`
- Menempelkan file certificate di virtual host

```
# cp /etc/apache2/sites-available/default /etc/apache2/sites-available/ssl
```

- edit file `/etc/apache2/sites-available/ssl`, tambahkan script pada baris terakhir sebelum `</VirtualHost>` :

SSL Engine On

```
SSLCertificateFile /etc/apache2/ssl/apache.pem
```

dan port default 80 dijadikan 443, cari baris `<VirtualHost *:80>` dan ganti dengan `<VirtualHost *:443>`

- edit file `/etc/apache2/sites-available/default`, tambahkan script pada baris terakhir sebelum `</VirtualHost>` :

```
SSLCertificateFile /etc/apache2/ssl/apache.pem
```

- Lakukan restart apache2 dan aktifkan modul HTTPS :

```
# /etc/init.d/apache2 force-reload
```

```
# a2ensite ssl
```

- Terakhir restart kembali apache2 :

```
# /etc/init.d/apache2 restart
```

2.3 Instalasi Email Server

2.3.1 Dovecot

Berikut ini adalah langkah-langkah instalasi Dovecot:

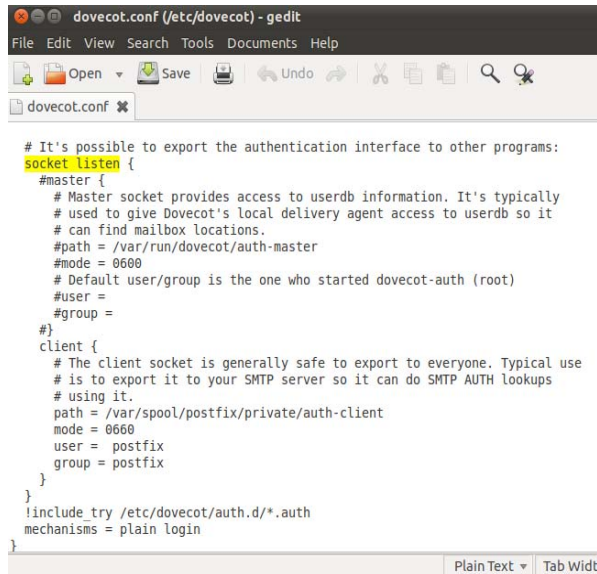
- Untuk mengunduh dan install Dovecot ketik `sudo apt-get install dovecot dovecot-common dovecot-imapd dovecot-pop3d`
- Lakukan konfigurasi pada dovecot ketik `sudo gedit /etc/dovecot/dovecot.conf`
- Tambahkan protocol imap dan pop3 pada file konfigurasi dovecot.

```
# Protocols we want to be serving: imap imaps pop3 pop3s managesieve
# If you only want to use dovecot-auth, you can set this to "none".
#protocols = imap imaps
protocols = imap pop3
```

- Setting Mailbox pada dovecot

```
#
# mail_location = maildir:~/Maildir
# mail_location = mbox:~/mail:INBOX=/var/mail/%u
# mail_location = mbox:/var/mail/%d/%n:INDEX=/var/indexes/%d/%n/%n
#
# </usr/share/doc/dovecot-common/wiki/MailLocation.txt>
#
#mail_location =
```

- Setting SASL untuk otentifikasi user dengan menghapus tanda '#' pada file konfigurasi di frase client pada socket listen.

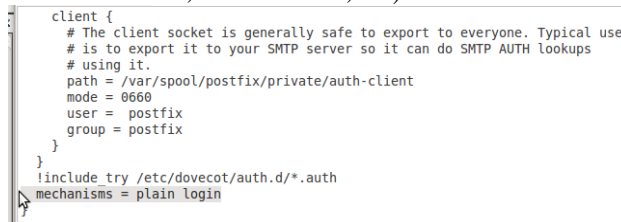


```

# It's possible to export the authentication interface to other programs:
socket listen {
#master {
# Master socket provides access to userdb information. It's typically
# used to give Dovecot's local delivery agent access to userdb so it
# can find mailbox locations.
#path = /var/run/dovecot/auth-master
#mode = 0660
# Default user/group is the one who started dovecot-auth (root)
#user =
#group =
#}
client {
# The client socket is generally safe to export to everyone. Typical use
# is to export it to your SMTP server so it can do SMTP AUTH lookups
# using it.
path = /var/spool/postfix/private/auth-client
mode = 0660
user = postfix
group = postfix
}
}
!include_try /etc/dovecot/auth.d/*.auth
mechanisms = plain login
    
```

Gambar 2. Setting SASL

- Tambahkan kalimat *mechanisms = plain login* pada file konfigurasi. Hal ini dimaksudkan agar IMAP Server (dovecot) dapat diakses oleh email client (mis : Thunderbird, Evolution Mail, Ms. Outlook, dll)

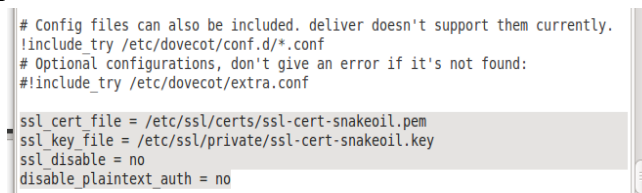


```

client {
# The client socket is generally safe to export to everyone. Typical use
# is to export it to your SMTP server so it can do SMTP AUTH lookups
# using it.
path = /var/spool/postfix/private/auth-client
mode = 0660
user = postfix
group = postfix
}
}
!include_try /etc/dovecot/auth.d/*.auth
mechanisms = plain login
    
```

Gambar 3. File Konfigurasi

- Aktifkan keamanan SSL pada dovecot dengan menambahkan perintah pada file konfigurasi



```

# Config files can also be included, deliver doesn't support them currently.
!include_try /etc/dovecot/conf.d/*.conf
# Optional configurations, don't give an error if it's not found:
#!include_try /etc/dovecot/extra.conf

ssl_cert_file = /etc/ssl/certs/ssl-cert-snakeoil.pem
ssl_key_file = /etc/ssl/private/ssl-cert-snakeoil.key
ssl_disable = no
disable_plaintext_auth = no
    
```

Gambar 4. Keamanan SSL

2.3.2 Postfix

Berikut ini adalah langkah-langkah instalasi Dovecot:

- Ketik `sudo apt-get install postfix` pada terminal.
- Lakukan konfigurasi pada postfix ketika `sudo dpkg-reconfigure postfix`
- Setting nama email server, tujuan pengiriman email, IP jaringan pada dialog tersebut.

2.4 Instalasi Webmail

Berikut ini adalah langkah-langkah instalasi Squirrel mail:

- Ketik *apt-get install squirrelmail-squirrelmail-decode* pada terminal.
- Tambah konfigurasi Squirrelmail pada Web Server (Apache)
cp /etc/squirrelmail/apache.conf /etc/apache2/conf.d/squirrelmail.conf
- Lakukan konfigurasi pada squirrelmail
/usr/sbin/squirrelmail-config. Maka akan muncul tampilan sebagai berikut:

```
SquirrelMail Configuration : Read: config.php (1.4.0)
-----
Main Menu --
1. Organization Preferences
2. Server Settings
3. Folder Defaults
4. General Options
5. Themes
6. Address Books
7. Message of the Day (MOTD)
8. Plugins
9. Database
10. Languages

D. Set pre-defined settings for specific IMAP servers

C Turn color on
S Save data
Q Quit

Command >> [ ]
```

Gambar 5. Konfigurasi Squirrelmail

- Edit nama domain dengan menekan angka 2, tekan 1 untuk merubah, tekan S untuk Simpan dan Q untuk keluar

```
SquirrelMail Configuration : Read: config.php (1.4.0)
-----
Server Settings

General
-----
1. Domain : compsecurity.org
2. Invert Time : false
3. Sendmail or SMTP : SMTP

A. Update IMAP Settings : localhost:143 (other)
B. Update SMTP Settings : localhost:25

R Return to Main Menu
C Turn color on
S Save data
Q Quit

Command >> [ ]
```

Gambar 6. Edit Domain

2.5 Instalasi MailScanner

MailScanner merupakan aplikasi untuk memeriksa keamanan dari email yang akan masuk dan yang akan dikirim. Di dalamnya sudah terintegrasi anti spam (SpamAssassin) dan antivirus (ClamAV).

1. Untuk mengunduh dan install Library dan Dependency MailScanner ketik
apt-get install libconvert-tnef-perl libdbd-sqlite3-perl libfilesys-df-perllibmailtools-perllibmime-tools-perllibmime-perllibnet-cidr-perllibsys-syslog-perllibio-stringy-perllibfile-temp-perl
2. Kemudian unduh dan install MailScanner ketik *apt-get install mailscanner*
3. Lakukan update pada database virus ClamAV ketik *sudo freshclam*
4. Untuk melakukan Stop layanan smtp pada server ketik *sudo /etc/init.d/postfix stop*
5. Buat direktori spam assasin ketik *mkdir /var/spool/MailScanner/spamassassin*
chown postfix /var/spool/MailScanner/spamassassin
6. Untuk melakukan edit konfigurasi pada MailScanner ketik *sudo edit /etc/MailScanner/MailScanner.conf*
7. setting parameter nama website, smtp, antivirus, dan anti spam

```

%org-name% = computer security
%org-long-name% = keamanankomputer
%web-site% = compsecurity.org
Run As User = postfix
Run As Group = postfix
Incoming Queue Dir = /var/spool/postfix/hold
Outgoing Queue Dir = /var/spool/postfix/incoming
MTA = postfix
Virus Scanners = clamav
Spam List = SBL+XBL
SpamAssassin User State Dir = /var/spool/MailScanner/spamassassin

```

8. Tambahkan parameter header checks pada postfix
`postconf -e "header_checks = regexp:/etc/postfix/header_checks"`
9. Edit file header_checks
`sudo /etc/postfix/header_checks`
10. Tambahkan parameter berikut
`^Received:/ HOLD`
11. restart mailscaannerdan postfix
`/etc/init.d/maillscanner start`
`/etc/init.d/postfix start`

2.6 Integrasi GnuPG pada Email Client

2.6.1 OpenPGP pada Squirrelmail

1. Unduh Plugin OpenPGP pada website plugin squirrelmail
2. Copy dan ekstrak unduhan OpenPGP ke direktori plugin squirrelmail
`#cp gpg-2.1.tar.gz #/usr/share/squirrelmail/plugins/`
`#tar -zxvf gpg-2.1.tar.gz`
3. Tambahkan plugin OpenPGP pada konfigurasi plugin squirrelmail
`#/usr/sbin/squirrelmail-configure`
4. Pilih 8 untuk masuk ke menu plugin dan pilih gpg

2.6.2 Enigmail pada Thunderbird

Install Enigmail dengan mengetikkan perintah `apt-get install enigmail` pada terminal.

3.6.3 GnuPG pada Mutt

Edit file konfigurasi pada Mutt dengan perintah `sudo gedit /etc/Muttrc` dan tambahkan parameter dibawah ini.

```

# GnuPG configuration
set pgp_decode_command="gpg --charset utf-8 --status-fd=2 %?p?--passphrase-fd 0? -
-no-verbose --quiet --batch --output - %f"
set pgp_verify_command="gpg --status-fd=2 --no-verbose --quiet --batch --output - --
verify %s %f"
set pgp_decrypt_command="gpg --status-fd=2 %?p?--passphrase-fd 0? --no-verbose --
quiet --batch --output - %f"
set pgp_sign_command="gpg --no-verbose --batch --quiet --output - %?p?--
passphrase-fd 0? --armor --detach-sign --textmode %?a?-u %a? %f"
set pgp_clearsign_command="gpg --charset utf-8 --no-verbose --batch --quiet --output
-%?p?--passphrase-fd 0? --armor --textmode --clearsign %?a?-u %a? %f"
set pgp_encrypt_only_command="/usr/lib/mutt/pgpwrappgpg --charset utf-8 --batch --
quiet --no-verbose --output - --encrypt --textmode --armor --always-trust -- -r %r -- %f"

```

```
set pgp_encrypt_sign_command="/usr/lib/mutt/pgpwrappgpg --charset utf-8 %?p?--  
passphrase-fd 0? --batch --quiet --no-verbose --textmode --output - --encrypt --sign  
%?a?-u %a? --armor --always-trust -- -r %r -- %f"  
set pgp_import_command="gpg --no-verbose --import %f"  
set pgp_export_command="gpg --no-verbose --export --armor %r"  
set pgp_verify_key_command="gpg --verbose --batch --fingerprint --check-sigs %r"  
set pgp_list_pubring_command="gpg --no-verbose --batch --quiet --with-colons --list-  
keys %r"  
set pgp_list_secring_command="gpg --no-verbose --batch --quiet --with-colons --list-  
secret-keys %r"  
set pgp_good_sign="^\[GNUPG:\] GOODSIG"
```

3. HASIL DAN PEMBAHASAN

Saat berkomunikasi atau berbagi informasi melalui email, tidak jarang kita menyertakan data-data seperti email, username, password atau informasi sensitif lainnya. Untuk melindungi isi email yang sifatnya rahasia tersebut, maka dapat menggunakan fitur **PGP**. PGP digunakan untuk mengenkripsi body isi pesan email. Dengan menggunakan metode ini maka proses pertukaran informasi membutuhkan persetujuan sebelumnya antara pihak pengirim dan pihak penerima dengan melakukan pertukaran "*public key*" sehingga isi pesan jauh lebih terjamin kerahasiaannya.

Dalam penelitian ini menggunakan perangkat lunak *GnuPG* yang diintegrasikan dengan mail client *Thunderbird*. Author memilih Thunderbird sebagai mail client karena ia tersedia di berbagai macam **OS**.

Dengan sistem ini kita dapat :

- Mengatur beberapa akun email melalui satu program
- Menggunakan kunci enkripsi umum untuk menjaga privasi email
- *Enigmail* berbasis ***kunci publik kriptografi (public-key cryptography)***. Di metode ini, setiap individu harus mendapatkan kunci pasangan pribadi (*personal key pair*) mereka. Kunci pertama disebut *kunci pribadi (private key)*. Kunci ini dilindungi oleh kata sandi atau kalimat rahasia
- Dengan *Enigmail*, juga dapat melampirkan tanda tangan digital dalam pesan. Penerima pesan yang memiliki salinan kopi asli dari *kunci publik* akan dapat memverifikasi bahwa asal email tersebut darimana, dan isi dari email tersebut belum diketahui oleh siapapun..

Mengamankan data pribadi sangat diperlukan di era saat ini, salah satu caranya adalah dengan melakukan enkripsi data.

Selain untuk melakukan enkripsi, GPG bisa juga digunakan untuk melakukan *signing* file atau dokumen sehingga bisa dipastikan apakah dokumen tersebut benar berasal dari pengirimnya atau bukan. Karena GPG menggunakan enkripsi Public Key maka diperlukan 2 (dua) buah kunci untuk melakukan sebuah enkripsi, yaitu:

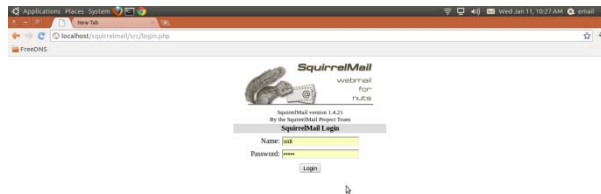
1. **Kunci privat** - kunci yang pertama kali dibuat, dan merupakan **identitas** yang sangat rahasia dan tidak boleh disimpan sembarangan.

2. **kunci publik** - kunci yang diberikan kepada lawan bicara agar bisa melakukan enkripsi dan mengirimkan email.

Pada sistem ini Email akan dikirim melalui webmail(Squirrelmail) dengan dienkripsi sebanyak dua kali, yaitu dengan GnuPG dan dienkripsi lagi saat ditransfer melalui protocol https, sehingga terjaga kerasiannya.

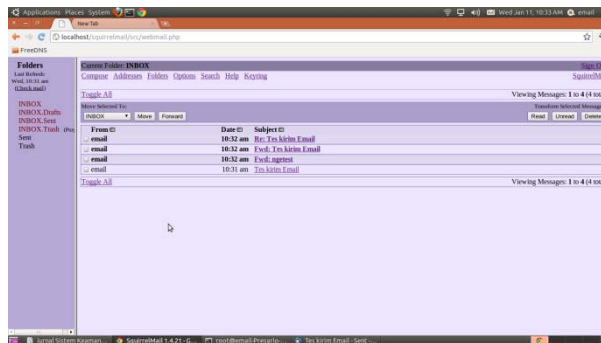
Berikut tampilan dari email server yang sudah dapat digunakan.

Tampilan Login



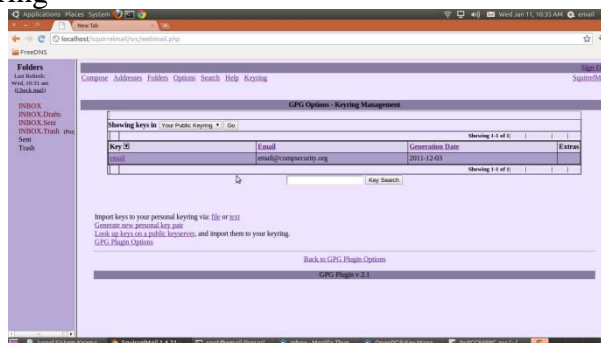
Gambar 7. Menu Login

Tampilan Inbox



Gambar 8. Inbox

Tampilan GPG Keyring



Gambar 8. GPG Keyring

4. KESIMPULAN

Dari hasil pembahasan tentang pembuatan sistem keamanan email menggunakan GnuPG, maka dapat diambil kesimpulan.

- Pengguna dapat mengirim email dengan aman karena email dapat dienkripsi.
- Pengirim dapat menandatangani email sehingga penerima yakin bahwa email yang diterimanya adalah asli dari pengirim email.
- Hanya penerima yang sah dan memiliki private key yang dapat membaca email yang dienkripsi oleh pengirim email.
- Email yang dikirim melalui webmail(Squirrelmail) dienkripsi sebanyak 2x, yaitu dengan GnuPG dan dienkripsi lagi saat ditransfer melalui protocol https.

5. SARAN

Saran-saran untuk untuk penelitian lebih lanjut untuk menutup kekurangan penelitian. Tidak memuat saran-saran diluar untuk penelitian lanjut.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada redaksi jurnal Jupiter yang telah memuat artikel ini dalam jurnal.

DAFTAR PUSTAKA

- [1] Erkarth, Hattenstar, 2014, The GnuPG Made Easy, <https://www.gnupg.org/documentation/manuals/gpgme.pdf>, diakses 12 Oktober 2015
- [2] B Price, 2010, Downloading and Using Mozilla Thunderbird, <https://www.ischool.utexas.edu/thunderbird.pdf>, diakses 12 Oktober 2015
- [3] Chyntia Irine Oroh, Webmail Server Squirrelmail, <http://www.squirrelmail.>, diakses 03 Oktober 2015