ANALISIS KEAMANAN PENGIRIMAN EMAIL MENGGUNAKAN WinPT (*Windows Privacy Tray*)

Bofandra – NIM : 13506043

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if16043@students.if.itb.ac.id

Abstrak

Kirim-mengirim email (surat elektronik) seringkali kita lakukan pada saat sekarang ini. Tanpa kita sadari, kerahasiaan pesan yang kita kirimkan atau yang kita terima, terancam oleh perilaku oknum-oknum yang tidak bertanggung jawab. Pada makalah ini, Penulis akan menganalisis keamanan pengiriman email menggunakan aplikasi WinPT (*Windows Privacy Tray*). Aplikasi WinPT adalah sebuah aplikasi *open source* dalam bidang kriptografi. Aplikasi ini menggunakan algoritma kriptografi kunci publik dalam meng-en-dekripsi pesan. Penulis berharap, makalah ini, dapat menambah pengetahuan pembaca mengenai aplikasi WinPT, termasuk menemukan kelebihan dan kekurangannya, khususnya dalam hal keamanan pesan.

***Kata kunci**: e-mail, WinPT*, kriptografi, kunci publik, keamanan pesan

1. Latar Belakang

Keamanan dalam kirim mengirim email adalah kebutuhan sehari-hari pada saat sekarang ini. Kebutuhan ini baru terasa betul, ketika pesan yang akan kita kirimkan sangat penting dan rahasia.

Ternyata, telah ada aplikasi (*software*) yang menjawab tantangan ini. Salah satunya adalah WinPT. Aplikasi ini berbasis *open source*, sehingga dapat digunakan secara gratis. Selain itu, dengan disebarluaskannya *source code* aplikasi ini, memberikan kesempatan bagi orang-orang, termasuk Penulis, untuk mempelajarinya.

2. Tujuan

Tujuan dari penulisan makalah ini, antara lain :

1) Memberikan informasi kepada pembaca mengenai WinPT
2) Mengetahui tingkat keamanan pengiriman email menggunakan aplikasi WinPT

3. Perumusan Masalah

Secara garis besar, makalah ini akan melingkupi hal-hal sebagai berikut :

1) Aplikasi WinPT secara garis besar
2) Cara penggunaan aplikasi WinPT untuk pengiriman email
3) Studi kasus untuk mengetahui tingkat keamanan pengiriman email menggunakan aplikasi WinPT

4. Pembahasan

4.1. WinPT

WinPT adalah sebuah kakas kriptografi yang merupakan *GUI* dari *Gnu Privacy Guard* (GnuPG). WinPT dikhususkan untuk pengguna yang menggunakan *platform* Windows.

WinPT memiliki fitur-fitur sbb.

1) *Key Generator*
2) *Key Manager*
3) *File Manager*
4) Enkripsi dan dekripsi

5) Tanda-tangan digital
6) Import kunci publik dari website

4.2. Pengiriman Email Menggunakan WinPT

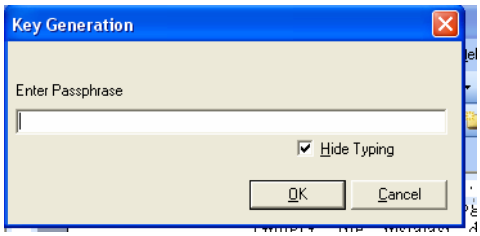
Jika belum memiliki program WinPT maupun GnuPG, file instalasi dapat diperoleh dari http://www.gpg4win.org/download.html. Proses instalasi dapat dilakukan dengan mudah karena telah ada *wizard* yang akan memandu

Langkah-langkah pengiriman *email* menggunakan WinPT adalah sbb.

a. Pengirim *email* maupun penerima *email* men-*generate* kunci publik dan kunci privat mereka masing-masing

Pertama kali program WinPT dijalankan, program akan menjalankan *Key Generation Wizard*.

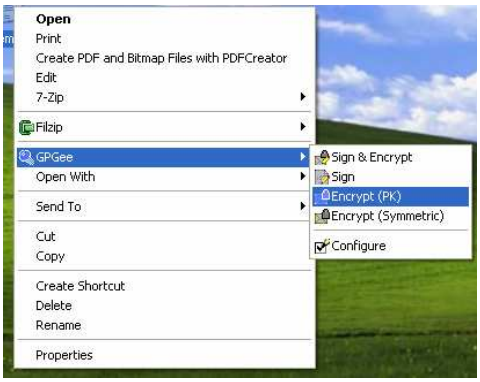
Setelah mengetikan *Real Name* dan *Email address* pada tempat yang disediakan, program akan kembali meminta pengguna memasukkan data yang lain, yaitu : *Passphrase*. *Passphrase* ini juga dapat berlaku sebagai kunci privat dalam enkripsi/ dekripsi.



Setelah itu, program akan men-*generate* kunci (kunci publik dan kunci privat). Kunci yang telah dihasilkan dapat kita simpan (*backup*) agar tidak terjadi kehilangan.

b. Pengirim *email* men-enkripsi email yang akan dikirim

Tulis *email* pada sebuah file (misal) tipe teks file. Lalu klik kanan pada file yang telah dibuat tersebut.



Pilih Encrypt (PK) untuk meng-enkripsi menggunakan teknik *Public Key*.

Secara *default* program akan memilihkan opsi *Signature* : None dan Opsi *Encryption* : Public-key. Pilih opsi *Signature* : *Attached* jika ingin menambahkan tanda-tangan-digital pada email.

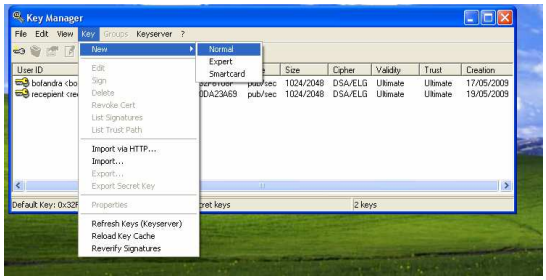
Pada daftar *Encryption Key Selection* terdapat *Public-key* dari calon-calon penerima email.

Klik pada *Checkbox* calon penerima yang dipilih, lalu klik *Ok*. Pada folder yang sama dengan file email kita tadi, akan muncul satu file baru berekstensi .gpg. File inilah yang selanjutnya akan dikirimkan ke penerima.

Jika belum terdapat *public key* dari calon penerima yang ingin kita kirimkan *email* pada daftar *Encryption Key Selection*, maka kita dapat menambahkannya dengan cara :

- Klik kanan pada windows tray WinPT lalu pilih *Key Manager*

- Maka akan muncul kotak dialog *Key* Manager, pilih menu Key > New > Normal



- Maka akan muncul *Key Generation Wizard* seperti pada penjelasan poin **1** (Pengirim *email* maupun penerima *email* men-*generate* kunci publik dan kunci privat mereka masing-masing)

c. Penerima *email* men-dekripsi *email* yang telah diterima

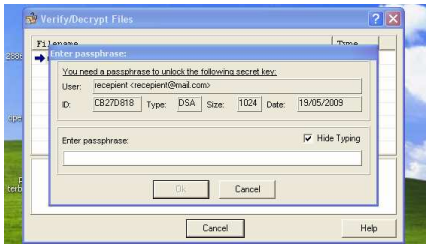
.

Sebelumnya, penerima juga harus telah meng-*install* program WinPT pada komputernya.

Email yang telah diterima dapat didekripsi kembali dengan cara sbb.

Klik kanan pada berkas email (berekstensi .gpg), lalu pilih *Verivy/ Decrypt*.

Kemudian akan muncul kotak dialog Verivy/ Decrypt Files, serta program akan meminta pengguna (dalam hal ini : penerima email) untuk memasukkan *pharaphrase*. *Pharaphrase* ini adalah kunci privat dari penerima email.



Setelah *pharaphrase* diketikkan dan tombol *Ok* ditekan, maka program akan otomatis men-*generate* file hasil dekripsi pada folder (lokasi) yang sama dengan *email* awal (sebelum didekripsi).

4.3. Tingkat Keamanan Pengiriman Email Menggunakan WinPT

Beberapa serangan yang mungkin terjadi pada kirim-mengirim *email* menggunakan WinPT antara lain :

a. Pihak penyerang mencari kesempatan untuk melihat pengguna WinPT ketika mengetikkan *pharaphrase*
b. Pihak penyerang membuat *website* atau program yang mirip dengan WinPT, sehingga pengguna menjadi tertipu
c. Pihak penyerang membuat *account user* pada program WinPT dengan nama yang mirip dengan seorang pengguna yang menjadi terget (*victim*)

5. Kesimpulan

Melihat kemungkinan-kemungkinan serangan pada aplikasi WinPT, dibandingkan dengan kemudahan yang ditawarkan aplikasi ini, WinPT masih dapat dikatakan cukup baik dalam menjaga kerahasiaan suatu pesan. Hanya saja pengguna harus lebih berhati-hati dalam menggunakannya.

DAFTAR PUSTAKA

[1] Munir, Rinaldi. (2004). Bahan Kuliah IF5054 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung.

[2] http://winpt.gnupt.de/winpt.en.zip. Tanggal Akses : 7 Mei 2009

[3]http://www.securityfocus.com/archive/1/archive/1/471045/100/0/threaded. Tanggal akses : 21 Mei 2009