

Pengamanan Sistem Berkas

Jutono G
Fakultas Ilmu Komputer Universitas AKI

Abstract

The more important and the higher the value of data that are processed and stored in information technology, the more people try to access, break, or even use the data. Because of that the protection for data security is very essential. Techniques used to protect the data are classified into three methods, those are Attribute Keying, Compression Keying and Encryption. Those techniques are being developed regarding to the need of data security and information technology development. This paper is expected to give contribution toward security system for high confidential data.

Key words: *data security, attribute keying, compression keying, encryption, information technology development*

Pendahuluan

Keamanan komputer adalah suatu cara untuk mencegah penyerang yang tidak mempunyai hak akses dan tidak mempunyai hak pakai terhadap sistem komputer dan jaringan (John D. Howard,1995). Keamanan ini bertujuan agar pemilik sistem informasi dapat menjaga sistem informasinya tidak disusupi oleh orang lain yang pada akhirnya dapat merusak sistem. Adapun tujuan dari penyusup ini dapat berupa :

a. *The Curious*, dimana penyusup hanya sekedar ingin tahu tentang sistem dan data yang ada.

b. *The Malicious*, dimana penyusup hanya merubah bentuk tampilan dan mengacak-acak sistem sehingga menjadi down, sehingga pemilik sistem mengeluarkan uang untuk memperbaiki sistemnya.

c. *The High-Profile Intruder*, dimana penyusup bertujuan untuk mencari popularitas.

d. *The Competition*, dimana penyusup sudah memanfaatkan sistem komputer yang disusupnya untuk keuntungan pribadi.

Dari tujuan penyusup dapat dipahami bahwa sistem keamanan komputer

merupakan salah satu aspek penting dari sebuah sistem informasi. Tapi sangat disayangkan masalah ini sering kali kurang mendapat perhatian dari pada pemilik dan pengelola sistem informasi. Dan seringkali masalah keamanan menjadi urutan yang kedua bahkan terakhir dalam prioritas hal-hal penting pada sistem informasi pada hal sistem informasi sudah menjadi *information-based society*. Berikut ini adalah beberapa contoh kegiatan yang dapat anda lakukan jika sistem anda dirusak, seperti :

1. Hitung kerugian apabila sistem informasi anda tidak bekerja selama 1 jam, selama 1 hari, selama 1 minggu dan selama 1 bulan.
2. Hitung kerugian apabila ada kesalahan informasi (data) pada sistem informasi anda. Misalnya web site anda mengumumkan harga sebuah barang yang berbeda dengan harga yang ada di toko anda.
3. Hitung kerugian apabila ada data yang hilang, misalnya daftar pelanggan yang hilang, bahan-bahan kuliah yang hilang, soal ujian yang disabot, dan lain-lain.

Dibawah ini merupakan sedikit catatan atau statistik kerusakan sistem informasi yang disebabkan bobolnya keamanan sistem, seperti :

- Di Inggris, 1996 *NCC Information Security Breaches Survey* melaporkan rata-rata perusahaan kerugian US \$30.000,- untuk 1 kali perbaikan sistem informasinya yang rusak di bobol oleh penyusup (cracker).
- Winter 1999, *Computer Security Institute* dan FBI (<http://www.gocsi.com>) melaporkan hasil surveinya dari responden pemakai sistem informasi ; 62% dalam 12 bulan terakhir, sistemnya digunakan oleh orang yang tidak berhak (*unauthorized users*), 86% serangan berasal dari dalam sistem sendiri dan 74% serangan dari hackers.
- 1988, Keamanan sistem mail Sendmail dieksploitasi oleh Robert Tapan Morris sehingga melumpuhkan Internet dengan serangan *Denial of service attack (DoS)* sehingga data-data e-mail (*elektronik mail*) pelanggan tidak dapat diakses. Dan untuk memperbaiki sistem sendmail dibutuhkan dana US \$ 100 juta dan 1990 Morris dihukum hanya US \$ 10.000,- (karena lemahnya hukum di bidang Sistem Informasi).
- 10 Maret 1997, seorang hacker dari Massachusetts berhasil mematikan sistem telekomunikasi di sebuah airport Worcester, Massachusetts dan

menghalau semua pesawat yang hendak mendarat.

Dan masih banyak yang lain (<http://www.2600.com>), tapi tidak semua perusahaan melaporkan atas kebobolan sistem informasinya, karena dapat menyebabkan pandangan negatif dari masyarakat umum (*negative publicity*), sehingga banyak yang memilih untuk diam dan mencoba menangani sendiri. Untuk itu kita harus mencegah penipuan (*cheating*) atau paling tidak mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik (G.J. Simons, 1995).

Metoda Pengamanan

Menghadapi ancaman (*managing threats*) terhadap sistem keamanan komputer dapat digunakan suatu model yaitu Risk Management Model (Lawrie Brown, 1995). Manajemen ini membagi 3 (tiga) komponen yang dapat memberikan kontribusi terhadap Risk, yaitu :

- Aset (*assets*), yaitu pemilik sistem informasi harus mendiskripsikan segala kekayaan pada sistem dan memperhitungkan segala resiko yang akan timbul dari kegagalan terhadap salah satu komponen tersebut, seperti : *hardware*, *software*, dokumentasi, data, komunikasi, lingkungan, manusia

- Ancaman (*threats*), yaitu mendeskripsikan semua ancaman yang akan terjadi terhadap sistem, seperti : pemakai (*users*), teroris, kecelakaan (*accidents*), crackers, penjahat criminal, nasib (*acts of God*), mata-mata (*foreign intellegence*)

- Kelemahaan (*Vulnerabilities*), yaitu mendiskripsikan semua kelemahan yang ada pada sistem, seperti : *software bugs*, *hardware bugs*, radiasi (layar monitor, transmisi), *crossstalk*, *unauthorized users*, cetakkan, *hard copy*, atau *print out*, keteledoran (*oversight*), *cracker* media penyimpanan

Dari banyaknya resiko yang akan dihadapi oleh suatu sistem informasi, semuanya itu merupakan hal yang sangat penting dan tidak dapat dianggap sepele. Salah satunya terhadap file data, yang merupakan suatu aset yang banyak digunakan dan selalu ada dalam suatu sistem informasi.

Metoda untuk mengamankan file data dapat dilakukan dengan 3 (tiga) cara, yaitu :

1. **Attribut Keying**, yaitu suatu penguncian terhadap attribut sebuah file data.

Setiap file data dalam sistem informasi (komputer) selalu diikuti oleh attribut file, yang berfungsi untuk mengamankan file agar tidak dapat diserang oleh orang lain. Attribut itu terdiri atas :

- R (*read*), yaitu penguncian atribut sehingga pemakai hanya dapat melakukan pembacaan saja terhadap isi file.
- W (*write*), yaitu penguncian atribut sehingga pemakai dapat melakukan penulisan (simpan) terhadap isi file.
- X atau A (*access*), yaitu penguncian atribut sehingga pemakai dapat melakukan pengaksesan (eksekusi) file.

Perintah penguncian ini dapat dilakukan dengan menggunakan perintah eksternal dari Sistem Operasi (*Operating System*) seperti :

- CLI (*Command Line Interface*) dalam *Disk Operating System* (DOS) dengan menggunakan perintah ATTRIB., seperti tampilan dibawah ini.

```
Displays or changes file attributes.

ATTRIB [+R|-R] [+A|-A] [+S|-S] [+H|-H]
      [[drive:] [path]filename]

+ Sets an attribute
- Clear an attribute
R Read only file attribute
A Archive file attribute
S System file attribute
H Hidden file attribute
/S Processes files in all directories
in the      specified path.
```

Gambar 1. Bentuk tampilan perintah ATTRIB pada DOS

Dan dalam Sistem Operasi Unix dengan menggunakan perintah CHMOD dengan bentuk tampilan seperti :

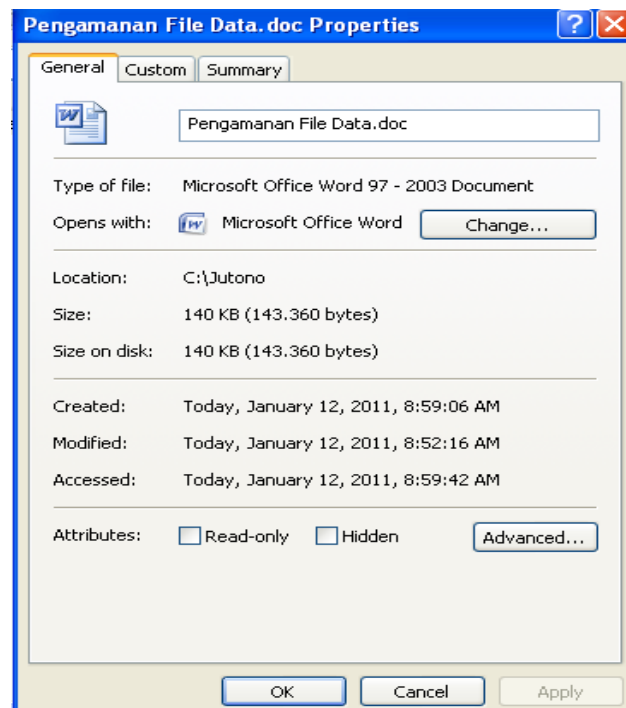
```

$chmod 755 mail
Hasilnya mode perizinan untuk file mail akan bertukar seperti
berikut:-
drwxr-xr-x 2 lithium sysadmin 512 Dec 10 18:51 mail
tabel nomor basis dalam perizinan adalah :
r w x
0 0 0 0
1 0 0 1
2 0 1 0
3 0 1 1
4 1 0 0
5 1 0 1
6 1 1 0
7 1 1 1

```

Gambar 2. Bentuk tampilan perintah CHMOD

- GUI (*Graphics User Interface*) dalam sistem operasi Windows dengan menggunakan perintah click File, Properties, General dan dapat dilihat pada gambar berikut:



Gambar 3. Bentuk tampilan Attrib pada Windows

2. Compress Keying, yaitu suatu penguncian terhadap hasil pemadatan file data.

Setiap file data dapat dirobah kedalam bentuk yang lebih padat dengan menggunakan aplikasi kompres, seperti RAR, ZIP dan lain-lain. Hasil dari kompres dapat di kunci dengan menambahkan Password (kata kunci) pembuka apabila file tersebut di decompress atau dikembalikan kedalam bentuk semula (*extract*).

Prinsip kerja dari kompres adalah mencari character atau byte yang sering atau banyak berada dalam sebuah file data. Karakter tersebut akan dirobah kedalam kumpulan bit yang lebih sedikit (kurang dari 8 bit).

Contoh :

Isi sebuah file adalah **AMANKAN DATA ANDA_**, yang berkapasitas 17 byte (space = byte) x 8 bit = 136 bit. Data tersebut terdiri atas 7 buah huruf A yang dalam bentuk biner 01000001. Untuk itu bentuk bit huruf A

dikompres kedalam bentuk bit yang terdiri atas 2 bit, sehingga file data tersebut hanya terdiri atas $7 \times 2 + 8 \times 10 = 94$ bit (11.75 byte).

3. Encryption (Enkripsi), yaitu merupakan suatu teknik merubah isi file data dengan bentuk rahasia yang tidak dimengerti oleh orang lain.

Cara kerja dari enkripsi dapat dilihat pada diagram dibawah ini :

Plain text > Enkripsi > Cipher text > Deskripsi > Plaintext

Yang disembarkankan bagi pemakai adalah bagian Cipher Text.

$$M = ROT13(ROT13(C))$$

Keterangan : M = Plain Text, C = Cipher Text

Salah satu contoh dari Enkripsi adalah ROT13, dengan rumus :

$$C = ROT13(M)$$

1	2	3	4	5	6	7	8	9	10	11	12	13
A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

14	15	16	17	18	19	20	21	22	23	24	25	26
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M

Misal :

M = AMANKAN DATA ANDA

C = NZNAXNA#QNGN#NAQN (space = #)

Salah satu software encryption yang populer saat ini adalah PGP (*Pretty Good Privacy*) yang dibuat oleh **Phill Zimmermann** tahun 1990.

Jenis-jenis proteksi data enkripsi terdiri atas :

- Teknik Substitusi (*Substitution Technique*), yaitu teknik yang melakukan proteksi data dengan cara menggantikan setiap elemen data atau karakter dengan karakter lain.
- Teknik Blok (*Blocking Technique*), yaitu teknik proteksi data dengan cara mengelompokkan beberapa karakter ke dalam blok-blok yang berisi beberapa karakter.
- Teknik Permutasi (*Permutation Technique*), yaitu teknik proteksi data dengan cara menukarkan letak karakter-karakter yang ada.
- Teknik Ekspansi (*Expansion Technique*), yaitu teknik proteksi data dengan cara menambahkan suatu karakter kedalam data.
- Teknik Pemadatan (*Compaction Technique*), yaitu teknik proteksi data dengan cara menghilangkan sejumlah karakter dalam data.

Kesimpulan

File data merupakan suatu komponen yang sangat penting dalam sistem informasi, sehingga jangan sampai terjadi kerusakan dan bahkan dibaca oleh orang lain yang tidak berhak (*unauthorized user*). Untuk itu file data harus diamankan untuk kelancaran dari suatu sistem informasi. Teknik pengamanan yang dapat dilakukan dapat berupa :

- Penguncian Atribut (*Attribut Keying*)
- Penguncian Kompres (*Compression Keying*)
- Diubah kedalam bentuk rahasia (*Encryption*)

Software – software untuk mendukung pengamanan ini sudah banyak disediakan oleh Sistem Operasi maupun Sistem Aplikasi yang berkembang pada saat ini, seperti :

- Attrib (aplikasi Atribut Keying)
- Chmod (aplikasi Atribut Keying)
- Rar (aplikasi Compress Keying)
- PGP (*Pretty Good Privacy*) (aplikasi Encryption)
- Dan lain-lain.

Disamping itu, juga dapat dibangun sendiri programnya dengan menggunakan bahasa pemrograman tingkat tinggi seperti Pascal, C++, Visual Basic, dan lain-lain.

Daftar Pustaka

Budi Rahardjo, *Keamanan Sistem Informasi: Beberapa Topik Keamanan di Internet*, Seminar Informasi Infrastruktur Nasional, ITB, 1997

Computer Security Institute, 1999 *CSI/FBI Computer Crime and Security Survey*,
CSI, Winter 1999.
<http://www.gocsi.com>

G.J Simson, dan gene Spafford, *Practical UNIX & Internet Security*, O'Reilly & Associates, Inc., 2nd edition, 1996

John D. Howard, *An Analysis of Security Incidents on the Internet 1989-1995*,
PhD thesis, Engineering and Public Policy, Carnegie Mellon University, 1997

Lawrie Brown, *Lecture Notes for Use with Network and Internetwork Security by William Stallings*,
on-line document.

<http://www1.shore.net/~ws/Security-Notes/index.html>

Onno W. Purbo, *Keamanan Jaringan Internet*,
Elex Media Komputindo, Jakarta, 2000

Simson Garfinkel, *PGP: Pretty Good Privacy*,
O'Reilly & Associates, Inc., 1995

William Stallings, *Network and Internetwork Security*,
Prentice Hall, 1995

www.2600.com

www.cert.org

www.bogor.net/idkf