



KILAT

JURNAL KAJIAN ILMU DAN TEKNOLOGI

Adhitya Ilham Ramdhani

Arief Suardi Nur Chairat

Dian Hartanti

Faisal Piliang;
Silvester Dian Handy Permana

Indah Handayasari;
Hamzah Mujahid

Iriansyah BM Sangadji

Karina Djunaidi

Ghoni Rosyiddin;
Kikim Mukiman

Rahma Farah Ningrum

Sarwo; Wiwit

Shinta Esabella;
Iskandar Fitri

Yessy Asri

ANALISA DAN PERANCANGAN *ELECTRONIC CUSTOMER RELATIONSHIP MANAGEMENT (E-CRM)* DALAM MENINGKATKAN LOYALITAS PELANGGAN PADA PT. PENTA ARTHA IMPRESSI

IMPLEMENTASI PENERAPAN METODE *SIX SIGMA* PADA PROSES PERAKITAN ELEKTRO MOTOR (STUDI KASUS: PT. TATUNG ELECTRIC INDONESIA)

PERANCANGAN APLIKASI PEMANTAU KEAMANAN BERDASARKAN PERGERAKAN MENGGUNAKAN KONEKSI EMAIL, HANDPHONE DAN VIDEO

STRATEGI OPTIMASI DALAM MENENTUKAN LINTASAN TERPENDEK *UNDIVIDED RAGNAROK ASSAULT PROBLEM (UNDIVIDED GAMES)*

EVALUASI DAMPAK BANGUNAN SEMENTARA ARRIVING SHAFT PADA PEMBANGUNAN TEROWONGAN PENGENDALI BANJIR (SUDETAN) KALI CILIWUNG KE KANAL BANJIR TIMUR

ANALISIS SURVEY TRACER STUDI PROGRAM STUDI TEKNIK INFORMATIKA STRATA 1 SEKOLAH TINGGI TEKNIK PLN TAHUN 2014

PERENCANAAN STRATEGI TI DAN PENERAPANNYA PADA KOMISI AKREDITASI RUMAH SAKIT

SISTEM ANTI VIRUS MENGGUNAKAN METODE *CYCLIC REDUNDANCY CHECKSUM-32 "GnR-AV"*

IMPLEMENTASI MANAJEMEN ASSET PADA TIANG DISTRIBUSI LISTRIK JARINGAN TEGANGAN RENDAH DAN JARINGAN TEGANGAN MENENGAH DENGAN MEMANFAATKAN APLIKASI QGIS (*QUANTUM GEOGRAPHIC INFORMATION SYSTEM*)

PERANCANGAN SISTEM BERBASIS *FUZZY LOGIC* UNTUK DEDUPLIKASI PENUNJANG KEPUTUSAN KELAYAKAN NASABAH PADA LEASING PT. CS FINANCE

ANALISA DAN PERANCANGAN INFRASTRUKTUR JARINGAN KOMPUTER UNTUK MENDUKUNG PENGEMBANGAN IMPLEMENTASI *ELECTRONIC GOVERNMENT* (STUDI KASUS PEMERINTAH KABUPATEN SUMBAWA BARAT)

PEMANFAATAN *WEB SERVICE* SEBAGAI INTEGRASI DATA PADA TATA LAKSANA LABORATORIUM KOMPUTER (STUDI KASUS LAB.KOMPUTER LANJUT INFORMATIKA STT-PLN)

ISSN 2089-1245



SEKOLAH TINGGI TEKNIK - PLN (STT-PLN)

KILAT	VOL.4	NO.2	HAL.120-218	OKTOBER 2015	ISSN 2089 - 1245
-------	-------	------	-------------	--------------	------------------

SISTEM ANTI VIRUS MENGGUNAKAN METODE CYCLIC REDUNDANCY CHECKSUM-32 "GnR-AV"

¹ GHONIY ROSYIDDIN, Teknik informatika, STMIK Bani Saleh

¹ ghonny.rosyidin.gh@hitachi-kenki.com

² KIKIM MUKIMAN, , Teknik informatika, STMIK Bani Saleh

² kikimmukiman@gmail.com

Abstrak

Virus komputer sifatnya dapat merusak misalnya dengan merusak data pada dokumen, membuat pengguna komputer merasa terganggu dengan keberadaannya dalam sebuah sistem komputer, maupun tidak menimbulkan efek merusak sama sekali. Antivirus atau Virus Protection Software adalah sebuah jenis perangkat lunak yang digunakan untuk mendeteksi dan menghapus virus komputer dari sistem komputer. Model proses perangkat lunak yang digunakan yaitu model proses Sekuensial Linier atau Waterfall. Model sekuensial linier mengusulkan sebuah pendekatan kepada perkembangan perangkat lunak yang sistematis dan sekuensial yang diawali pada tingkat dan kemajuan sistem pada seluruh analisis, desain, kode, pengujian, dan pemeliharaan. Perangkat lunak yang dihasilkan adalah Aplikasi Virus dan Antivirus. Aplikasi virus dapat disebut dengan Qvir, sedangkan untuk antivirus dapat disebut dengan AntQ. Qvir dibangun dengan bahasa pemrograman Delphi 7, sedangkan AntQ dibangun dengan bahasa pemrograman Visual Basic 6. Pengujian terhadap perangkat lunak dilakukan dengan metode blackbox. Tujuan dibuatnya anti virus ini yaitu untuk mengetahui celah yang berpotensi untuk dimanfaatkan virus yang dapat merusak keamanan sistem komputer yang digunakan, sedangkan tujuan dibuatnya antivirus ini yaitu untuk menutupi celah dari sistem komputer tersebut maupun celah yang belum ditangani oleh antivirus lainnya, agar virus tersebut tidak dapat masuk serta merusak sistem komputer tersebut.

Kata kunci : Qvir, AntQ, Virus, Antivirus, File, CRC32

Abstract

Computer viruses can damage the nature example by destroying the data on the document, make computer users feel disturbed by its presence in a computer system, and does not cause deleterious effects at all. Antivirus or Virus Protection Software is a type of software that is used to detect and remove computer viruses from the computer system. Software process models used are linear or sequential process model Waterfall. Linear sequential model proposes an approach to software development that is systematic and sequential starting at the level and progress of the whole system analysis, design, code, test, and maintenance. The resulting software is virus and antivirus applications. Virus application can be called with Qvir, while for the antivirus can be called with antq. Qvir built with Delphi 7, while antq built with Visual Basic 6. Testing of the software is done by the method of blackbox. The objective of this antiviral is to determine the gaps that have the potential to be used viruses that could undermine the security of computer systems that are used, while the purpose of the antivirus that is to cover the gap from the computer system and the gaps not addressed by other antivirus, so that the virus can not be entry and damage to the computer system

Keywords: Qvir, antq, Virus, Antivirus, CRC32

PENDAHULUAN

Virus komputer merupakan salah satu software komputer yang menjadi ancaman bagi keamanan sistem komputer. Virus komputer sebagai salah satu jenis infeksi elektronik, dapat menyebabkan kerusakan pada sistem komputer yang diserangnya. Para user yang komputernya diserang oleh virus akan merasa tidak nyaman terhadap keberadaan virus tersebut yang mungkin akan memperlambat kinerja atau bahkan menghilangkan beberapa fungsi dari komputer. Antivirus adalah sebuah jenis perangkat lunak yang digunakan untuk mengamankan, mendeteksi dan menghapus virus komputer dari sistem komputer. Antivirus disebut juga Virus Protection Software. Aplikasi ini dapat menentukan apakah sebuah sistem komputer telah terinfeksi dengan sebuah virus atau tidak. Umumnya, perangkat lunak ini berjalan di latar belakang (background) dan melakukan pemindaian terhadap semua berkas yang diakses (dibuka, dimodifikasi atau ketika disimpan).

Cyclic Redundancy Check (CRC) adalah salah satu fungsi hash yang dikembangkan untuk mendeteksi kerusakan data dalam proses transmisi ataupun penyimpanan. CRC menghasilkan suatu checksum yaitu suatu nilai dihasilkan dari fungsi hash-nya, dimana nilai inilah yang nantinya digunakan untuk mendeteksi error pada transmisi ataupun penyimpanan data. Nilai CRC dihitung dan digabungkan sebelum dilakukan transmisi data atau penyimpanan dan kemudian penerima akan melakukan verifikasi apakah data yang diterima tidak mengalami perubahan ataupun kerusakan.

Metode yang dapat dipakai user sebagai metode pada proses scanning salah satunya adalah metode Cyclic Redundancy Check 32 (CRC32). Sesuai dengan fungsi utama dari fungsi hashing, CRC32 berfungsi untuk mengambil penanda dari sebuah file yang nantinya akan dipakai sebagai acuan untuk memeriksa apakah suatu file adalah file virus atau bukan. Kecil sekali kemungkinan bahwa dua buah file mempunyai nilai CRC32 yang sama. Hal ini disebabkan perbedaan 1 bit saja pada file akan mengubah nilai CRC32 file tersebut. CRC32 hanya mengambil 32 bit dari sebuah file yang

dijadikan sebagai penanda file tersebut. Hal ini berbeda dengan metode MD5 yang mengambil 128 bit dari file. Keuntungan memakai CRC32 adalah karena hanya terdiri dari 32 bit sehingga mempercepat proses scanning.

METODE PENELITIAN

Algoritma CRC

Adanya suatu algoritma untuk pengecekan data ini dikarenakan pada dasarnya ketika suatu data disimpan atau ditransmisikan bisa saja terjadi kerusakan seperti karena noise ketika transmisi, atau karena software pengolah data atau bahkan karena hacker. Jadi CRC sangat berguna meskipun ada juga hacker yang bisa membobolnya. Cara kerja CRC sederhana sekali kalau dibandingkan program algoritma yang lainnya karena fungsinya yang sangat spesifik juga. CRC menggunakan perhitungan matematika terhadap sebuah bilangan yang disebut sebagai checksum. Yaitu perhitungan berdasarkan total bit yang hendak ditransmisikan atau disimpan.

Checksum merupakan penghitungan jumlah frame data yang akan ditransmisikan kemudian ditambahkan sebagai informasi dalam header atau trailer data tersebut. Jadi checksum sudah dimiliki tiap data dengan jumlah atau besar nilai checksum yang berbeda-beda sesuai besar kecil space data tersebut. Kemudian setelah ditransfer, aplikasi penerima data akan menghitung kembali checksum (jumlah frame data) apa nilainya berubah atau tetap. Dengan membandingkan nilai frame sebelum dan sesudah transmisi atau penyimpanan, diketahui data telah berubah atau tidak.

CRC tidak menjamin data dari ancaman modifikasi atau perlakuan yang bertujuan merubah data oleh para hacker, karena memang para hacker bisa saja memanipulasi perhitungan checksum data dan mengganti nilai checksumnya sesuai kehendak hacker untuk membodohi penerima.

Cyclic Redundancy Check (CRC) cara kerjanya dapat digambarkan sebagai berikut. Dengan adanya blok bit k-bit, atau pesan, transmitter mengirimkan suatu deretan n-bit data, disebut sebagai FCS (*Frame Check Sequence*). Sehingga frame yang dihasilkan

terdiri dari $k+n$ bit. $K+N$ Bit ini dapat dibagi dengan jelas oleh beberapa nomor yang sebelumnya sudah ditetapkan. Kemudian receiver membagi frame yang datang dengan nomor tersebut dan bila tidak ada sisanya berarti data benar dan tidak terjadi kerusakan transfer.

Ada dua cara perhitungan yaitu :

- Aritmatika**
Penjumlahan bilangan biner tanpa menghitung atau memperhatikan pembawanya, atau biasa dinamakan operasi X-OR (Extradiationary Operation)
- Polynomic**
Menyatakan semua nilai bilangan biner sebagai suatu polynomial dengan satu variable.

Checksum dan Fungsi Hashing CRC32

CRC32 adalah kepanjangan dari " *Cyclic Redundancy Code*" dan 32 melambangkan panjang checksum dalam bit. Algoritma CRC adalah cara yang lebih baik dan teruji untuk pengecekan *byte* dalam jumlah besar dari suatu file yang telah termodifikasi maupun tidak, jika dibandingkan dengan metode yang mengacu pada nama atau ukuran *file*. Algoritma ini mencari lewat seluruh jumlah *byte* dan menghasilkan angka 32 bit untuk menggambarkan isi file dan sangat kecil sekali kemungkinan dua *stream* dari *byte* yang berbeda mempunyai CRC yang sama. Algoritma CRC32 dapat diandalkan juga untuk mengecek *error* yang terjadi dalam urutan *byte*. Dengan CRC32 kemungkinan perubahan standar (penyimpangan dari penghitungan CRC terhadap file) yang terjadi dapat dikendalikan. Nilai CRC32 dari sebuah file adalah nilai yang didapat dengan memproses ukuran dan nama file dengan nilai tabel CRC32 yang telah distandardkan.

Implementasi CRC32 pada pendeteksian virus adalah virus dapat dikenali melalui banyak cara, dapat melalui nama file, ukuran atau dengan membongkar isi file dan menemukan penandanya. Ada beberapa kelemahan jika hanya mengenalinya dari nama file. Terkadang program virus tidak memakai nama asli dari virus itu sendiri. Misalnya virus Hallo.roro.htt memakai nama program pemicunya sysrv.exe. Sehingga mau tidak mau untuk mendeteksi program itu antivirus harus melihatnya melalui ukuran file.

Ukuran file pun belum menjamin bahwa file tersebut adalah virus. Bisa saja ukuran filenya sama tetapi programnya berbeda. Sehingga diperlukan metode lain untuk mengenali file virus. Pengenalan virus melalui nilai CRC32 nya merupakan cara yang lebih akurat dan efektif.

PEMBAHASAN

Layar Utama dan Langkahnya

Berikut adalah langkah untuk menampilkan layar utama :

- Buka folder dimana anda meletakkan file GnR-AV.exe
- Klik 2x file GnR-AV.exe, kemudian akan tampil layar utama
- Untuk memulai scan komputer pilih lokasi mana yang anda ingin scan di drive (C:), (D:) atau yang lainnya selanjutnya klik tombol Scan
- Untuk menghentikan scan klik tombol Stop



Gambar 1

Layar Utama

Pengujian Perangkat Lunak

Untuk mengetahui apakah perangkat lunak / program yang dibuat telah bekerja dengan baik atau belum, maka perlu adanya suatu kegiatan pengujian terhadap perangkat lunak yang dibuat. Dengan melakukan pengujian, kita juga dapat mengetahui kesalahan-kesalahan yang mungkin muncul dan memastikan semua fungsi / modul program dapat berjalan.



Gambar 2

Drive Yang Terinfeksi Virus

Pada Gambar di atas terdapat sebuah Drive E:\ yang sudah terinfeksi virus Duplikasi.vbs & Salaty.vbs. Ketika sudah di Scan dengan Gnr-AV maka terdeteksi, seperti gambar dibawah ini :



Gambar 3

File Virus Yang Terdeteksi

Pada nilai Checksum terdapat 2 file virus dengan nilai CRC yang sama (2AFAD5F8) ini berarti virus dengan nama Duplikasi.vbs menggandakan dirinya sendiri dengan memakai nama baru (Salaty.vb.)

Pengujian Terhadap File

Untuk melihat kemampuan / kinerja Gnr-AV, maka perlu diadakan suatu perbandingan terhadap perangkat lunak antivirus yang ada dipasaran. Perangkat lunak antivirus yang dipilih sebagai bahan perbandingan adalah perangkat lunak yang bersifat freeware (Gratis). Adapun perangkat lunak yang digunakan untuk perbandingan adalah :

- PCMAV
Diperoleh dari bonus CD PC Media dan dengan penggabungan dengan signature dari ClamAV, perangkat lunak ini tidak perlu diinstall di komputer.
- AVG Antivirus Free Edition
Didownload dari <http://www.grisoft.com>, signature telah terkompilasi sehingga tidak

bisa diupdate secara manual dan antivirus ini harus diinstall ke komputer.

- ARTAV
Didownload dari <http://www.artav-antivirus.com>.
- SMADAV
Didownload dari <http://www.smadav.net>,

Sebagai bahan untuk pengujian kecepatan scanning, maka digunakan hardisk yang ada di komputer dengan perincian sebagai berikut :

- Drive C:\ dengan kapasitas 9.39 GB, terpakai 5.51 GB
- Drive D:\ dengan kapasitas 9.22 GB, terpakai 4.68 GB
- Drive F:\ berupa removable disk dengan kapasitas 1 GB dan berisi file 661 KB.

Pengujian ini menggunakan stopwatch, adapun hasil dari pengujian waktu scan dapat dilihat pada tabel berikut :

Tabel 1
Perbandingan Waktu Scan

NO	NAMA ANTI VIRUS	WAKTU SCAN DRIVE C :	WAKTU SCAN DRIVE D :	WAKTU SCAN DRIVE F :
1	Gnr-AV	00:18:54	00:08:46	00:00:10
2	AVG Antivirus Free Edition	1:10:24	00:20:42	00:12:56
3	ARTAV	00:52:12	00:09:47	00:21:12
4	SMADAV	00:25:32	00:11:50	00:08:57
5	PCMAV	00:39:44	00:05:50	00:00:28

Worm Jenis Kloning

Worm jenis kloning adalah worm yang memiliki kemampuan kloning secara cepat dan efektif. Artinya dalam waktu yang relatif singkat Worm mampu menyebar dan menggandakan diri dalam jumlah yang sangat besar. Adapun isi dari contohnya di bawah ini :



Gambar 4

Isi Coding Kloning Hice.vbs

Buka notepad dan simpan dengan nama Kloning Hide ber-extension *.vbs.

Dibawah ini algoritma dari isi codingnya :

- on error resume next
set
xGudril=CreateObject("Scripting.FileSystemObject")
Bertujuan untuk error handle dan File System Object, apabila ada script yang error maka program akan tetap berjalan.
- set
elkloner=xGudril.OpenTextFile(Wscript.ScriptFullName)
skrnta=elkloner.ReadAll
elkloner.Close
Bertujuan untuk mendefinisikan sebuah variable penampung untuk membuka dan menampung seluruh isi dari script VBS Worm. Karena nantinya akan mengkloning isi script VBS Worm tersebut ke seluruh file-file hasil kloning atau semua file hasil kloning akan berisi sama dengan script VBS Worm.
- for r=1 to 10
Variable penampung dengan nama r dan beri dengan nilai 1 dan tentukan berapa banyak Worm akan di kloning.
- set
kloner=xGudril.CreateTextFile("\Worm_GnR" & r & ".vbs")
Hasil kloning yang sudah di buat di beri nama "Worm_GnR", untuk memberikan akhiran 1,2,3 dst sampai 10, maka perlu ditambahkan {variable pengulangan}& dalam definisi variable kloner.
- kloner.write skrnta
Script yang sudah di baca dan ditampung dalam variable krenta.

- kloner.close
Close variabel kloner
- set atributya=xGudril.GetFile("\Worm_GnR" & r & ".vbs")
atributya.attributes=3
Memberikan atribut 3 (Hidden dan Read Only)
- next
Di akhir perulangan sampai dengan r=10



Gambar 5

Hasil dari kloner terbentuk 10 file yang di Hide

KESIMPULAN DAN SARAN

Kesimpulan

Setelah dilakukan pengujian, algoritma CRC merupakan cara yang bagus dan teruji untuk pengecekan byte dalam jumlah besar dari suatu file telah termodifikasi maupun tidak. Algoritma ini mencari lewat seluruh jumlah byte dan menghasilkan angka 32 bit untuk menggambarkan isi file. Dengan sangat kecil sekali kemungkinan dua stream dari byte yang berbeda mempunyai CRC yang sama. Algoritma seperti ini sangat cocok untuk mendeteksi virus jenis worm, terutama yang mempunyai ekstensi *.exe.

Pengecekan dengan metode CRC32 hanya efektif digunakan pada virus yang belum menerapkan teknik polymorphis yaitu virus yang setiap saat merubah header filenya.

Dengan memakai file definisi virus terpisah dari menyertakan utilitas CRC32 Viewer, kita dapat menambahkan definisi virus setiap saat, yaitu ketika ada virus baru muncul. Ini merupakan nilai tambah tersendiri dibandingkan dengan antivirus pembajakan yaitu AVG dan AVIRA, sehingga virus yang baru muncul dapat cepat terdeteksi.

Engine Scannernya cepat dan ringan tidak terlalu memberatkan memory. Terbukti dalam pengujian mampu melakukan scanning file berukuran 150MB dalam waktu 30 detik, sedangkan ukuran file program utamanya hanya 416 kb.

Saran

Beberapa saran yang penulis berikan berdasarkan uji coba yang dilakukan untuk pengembangan aplikasi ini lebih lanjut adalah :

- a. Antivirus ini perlu ditingkatkan sensitifitasnya, karena bila terdapat perubahan dari header file virus dengan teknik polymorphis maka antivirus ini tidak dapat mendeteksinya, Fungsi ini masih rawan dari kesalahan analisa.
- b. Antivirus ini belum dilengkapi dengan fasilitas scanning virus yang aktif di startup, untuk pengembangan lebih lanjut dapat ditambahkan fasilitas ini.
- c. Maka dari itulah butuh penelitian lebih lanjut dengan menambahkan algoritma baru, fungsi, atau prosedur agar dapat mengembangkan dan memajukan kualitas aplikasi antivirus.

DAFTAR PUSTAKA

Buku

- Baskoro, Yudhi Arie. 2007. 365 Trik Registry Windows XP. Mediakita, Jakarta.
- Hadi, Rahadian. 2001. Pemrograman Windows Api dengan Microsoft Visual Basic. PT. Elex Media Komputindo, Jakarta.
- Resha, Ahlul Faradish. 2007. Membuat Virus dan Antivirus Lanjutan. Gava Media, Yogyakarta.
- Shadewa, Aat. 2007. Rahasia Membuat Anti Virus Menggunakan Visual Basic 6.0. DSI Publishing, Yogyakarta.
- Yusianto, Rindra. 2008. Computer Worm (Belajar Membuat Worm Mulai dari Nol). Neomedia, Semarang
- Wardana, 2008. Virus Kung Fu. Jasakom, Jakarta.

Internet

- Wijayanto, Sakti, Indra. 2007. Penggunaan CRC32 Dalam Integritas Data [terhubung berkala] www.informatika.org/~rinaldi/Kriptografi/2006-2007/Makalah2/Makalah-054.pdf