PERANCANGAN DAN IMPLEMENTASI ANTIVIRUS UPDATE MENGGUNAKAN UNIVERSAL PACKET UPDATE

Muchammad Aiman[1], Fazmah Arief Yulianto[2], Tri Brotoharsono[3]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

Abstrak

Melakukan pencarian virus (virus scanning) adalah sangat bergantung pada virus definition yang telah dikenali oleh perangkat lunak antivirus pada suatu sistem operasi. Dalam kenyataannya setiap perusahaan perangkat lunak antivirus berusaha untuk memperbarui virus definition-nya sendiri tanpa bantuan dari kalangan pengguna teknologi informasi yang lain. Hal ini perlu diperbaiki dengan menawarkan suatu pendekatan yang mengakomodasi bagi kalangan pengguna teknologi informasi dan programmer yang jumlahnya sangat banyak untuk dapat membuat virus definition dengan bentuk baku dan hasilnya juga dapat digunakan oleh beberapa perangkat lunak antivirus yang telah ada.

Universal Packet Update adalah suatu metode untuk memperbarui virus definition dengan cara membentuk virus definition yang bersifat universal yang dapat digunakan oleh perangkat lunak antivirus dengan menggunakan modul tambahan yang bernama addons. Perangkat lunak antivirus dengan bantuan addons akan melakukan proses download dan convert untuk mendapatkan update packet dari Universal Packet Update Server.

Analisis dari hasil penelitian Universal Packet Update pada antivirus update ini menunjukkan bahwa setiap perangkat lunak antivirus yang diujicobakan dapat memperbarui virus definition miliknya dengan melakukan update ke UPU Server dengan bantuan addons. Adapun addons hanya akan mengambil virus definition yang dapat diterima oleh masing-masing antivirus dan menolak setiap virus definition yang tidak memiliki bentuk yang benar.

Kata Kunci : universal packet update, addons, virus definition, virus signature.

Abstract

Virus Scanning is very depend on virus definition that have recognized by local antivirus on the operation system. Actually, each antivirus software company will try to renew its virus definitions without help of information system people or programmers. This condition need to be changed by new approach to accommodate the information system peoples and programmer to amount very large for helping to make virus definitions with standard form and its result can be used by existing antivirus software.

Universal Packet Update is a method to update virus definition by producing virus definitions in universal form that can be used by the antivirus software by the help of additional modul named with addons. The antivirus software with addons will perform two update process such as download process and convert process. Both are performed to get the update packet from Universal Packet Update Server.

The analysis of the result of Universal Packet Update research pointed that each antivirus software that is tested can renew its virus definition by updating to UPU Server with addons help. And addons will only get the virus definition that can be accepted by each antivirus software and will reject the false virus definition.

Keywords : universal packet update, addons, virus definition, virus signature

1. Pendahuluan

1.1 Latar belakang

Pada dasarnya mengatasi virus komputer adalah mendefinisikan kode virus dan melakukan penyebaran *virus definition* tersebut ke pengguna perangkat *antivirus*. Kedua hal ini yaitu pendefinisian virus baru dan penyebaran *virus definition* harus dilakukan dengan cepat dikarenakan pertumbuhan virus baru juga sangat cepat.
Kecepatan dalam memperbaharui *virus definition* harus terus dikembangkan. Cepatnya pertumbuhan virus ini sangat dipengaruhi dari pembuat virus yang jumlahnya sangat banyak. Pada kenyataannya, perusahaan *antivirus* bekerja sendiri untuk menemukan *virus definition* baru yang mana *virus definition* ini sebenarnya telah ditemukan juga oleh perusahaan yang lain. Hal ini menyebabkan penggunaan waktu yang tidak efisien oleh perusahaan *antivirus* untuk menemukan *virus definition* yang telah ditemukan oleh para staf dari perusahaan *antivirus* yang lain.
Universal Packet Update adalah metode yang diujicobakan untuk mengatasi ancaman dari pertumbuhan virus yang sangat cepat dengan meningkatkan pertumbuhan *virus definition*. Metode *Universal Packet Update* berusaha untuk memberikan pendekatan dan cara baru dalam mempercepat pengumpulan *virus definition* dari para pengguna, ahli, dan pembuat program *antivirus* atau teknologi informasi. Untuk melakukan penelitian *Universal Packet Update*, diperlukan perangkat lunak *antivirus*, UPU *Server*, dan *addons*. Definisi-*virus definition* baru akan disimpan di *Universal Packet Update Server* untuk kemudian dapat diambil oleh pengguna perangkat lunak *antivirus* dimana pada perangkat lunak *antivirus* tersebut telah ditambahkan modul baru untuk melakukan *Universal Packet Update*. Modul tambahan yang digunakan untuk membantu *update virus definition* ini dinamakan *addons*.
Ada dua hal yang dilakukan *addons*, yaitu mengunduh *universal packet* dari UPU *server* kemudian mengubahnya menjadi *virus definition* baru dan menyimpannya pada direktori lokal perangkat lunak *antivirus*.

1.2 Perumusan masalah

Permasalahan yang menjadi objek penelitian dan pengembangan dalam Tugas Akhir ini adalah bagaimana perancangan dan implementasi dari *Antivirus Update* dengan menggunakan *Universal Packet Update* pada perangkat lunak *antivirus*.

1.3 Tujuan

Tujuan dari Tugas Akhir ini adalah sebagai berikut :

1. Menentukan susunan *universal update packet* yang dapat diterima oleh perangkat lunak *antivirus* yang akan diujicobakan dengan melakukan penggabungan kolom-kolom *virus definition* yang dimiliki oleh setiap perangkat lunak *antivirus*.
2. Membuat rancangan *addons* yang akan menjadi modul tambahan pada masing-masing perangkat lunak *antivirus* yang diuji.

3. Melakukan implementasi dari rancangan *Universal Packet Update* pada dua perangkat lunak *antivirus* yaitu ClamAV *Antivirus* dan MyAV *Antivirus* sebagai suatu ujicoba kelayakan penerapan metode *Universal Packet Update* pada *antivirus* yang ada.
4. Melakukan analisis efektifitas dan efisiensi terhadap proses *update* pada perangkat lunak *antivirus* yang telah ditambah dengan *addons* dan performansi *server* dalam menangani permintaan *update* dari *client* perangkat lunak *antivirus.*

1.4 Batasan Masalah

Untuk menghindari meluasnya materi pembahasan Tugas Akhir ini, penulis memberikan batasan masalah sebagai berikut :

1. *Universal Packet* adalah suatu struktur baku untuk paket data *virus definition*, yang dianggap memenuhi kebutuhan dari perangkat lunak-perangkat lunak *antivirus.*
2. *Addons* adalah modul tambahan pada perangkat lunak *antivirus* yang akan melakukan *download* (mengunduh) dan *convert* (mengubah).
3. Proses *download* paket universal akan melibatkan *client* dan *server* dimana *client*-nya adalah kesatuan perangkat lunak *antivirus* dan *addons*, sedangkan *server*-nya adalah sebuah aplikasi *server Universal Packet Update* yang menggunakan protokol HTTP.
4. Perangkat lunak *antivirus* yang akan diujicobakan adalah Clam *Antivirus* dan MyAV yang memiliki *virus definition* yang berbeda.
5. *Virus definition* yang digunakan sebagai sumber penelitian adalah *virus definition* yang didapatkan dari *antivirus* ClamAV. Hal ini dikarenakan sulitnya mendapatkan susunan *virus definition* dari perangkat lunak *antivirus* lain yang bersifat *close-source*.

1.5 Metodologi penyelesaian masalah

Metodologi yang digunakan dalam penyelesaian Tugas Akhir ini adalah :

1. Studi literatur
   Pada tahap ini, difokuskan untuk mencari referensi berupa buku, jurnal, bacaan yang berhubungan dengan landasan teori dalam penyelesaian Tugas Akhir ini.
2. Pengumpulan data
   Mengumpulkan perangkat lunak *antivirus* Clam *Antivirus* dan MyAV beserta *source code*-nya dan *file-file virus definition* dari kedua perangkat lunak *antivirus* tersebut.
3. Perancangan Sistem
   Merancang sistem *Universal Packet Update* yang meliputi perancangan universal packet, perancangan *addonss*, dan prosedur *update* antara *client* perangkat lunak *antivirus* dan *server* paket universal.
4. Implementasi pada Perangkat Lunak
   Mengimplementasikan rancangan *Universal Packet Update* pada dua perangkat lunak *antivirus* sebagai *client*, yaitu Clam *Antivirus* dan MyAV, dan pada *server* paket universal.

5. Analisis Performansi
   Melakukan analisis pada kerja *addons* pada perangkat lunak *antivirus* dan kerja *server* dalam menangani permintaan *update* dari berbagai *client* perangkat lunak *antivirus*.
6. Pembuatan Laporan
   Penyimpulan dari perancangan, implementasi, dan hasil analisis dan pembuatan laporan Tugas Akhir.

6. Simpulan dan Saran

6.1 Simpulan

Dari hasil pengujian yang dilakukan terhadap sistem, dapat diambil lima kesimpulan yaitu sebagai berikut :

1. Semua *update packet* yang dibuat oleh UPU *Server* dapat diambil oleh perangkat lunak *antivirus* baik ClamAV maupun MyAV.
2. Tidak semua *virus definition* yang ada pada *update packet* dapat digunakan oleh perangkat lunak *antivirus* baik ClamAV maupun MyAV. Hal ini dipengaruhi dari jenis *virus definition* yang dapat diterima oleh masing-masing *antivirus.*
3. *Addons* pada ClamAV maupun MyAV berhasil melakukan tugasnya untuk melakukan *download* dan *convert* terhadap *update packet* yang diterima dari UPU Server dengan melakukan *error checking* pada *virus definition* yang rusak.
4. *Antivirus* yang memiliki bentuk *virus definition* lebih sedikit akan memiliki nilai *overhead* baris *virus definition* yang lebih besar sebagai biaya bagi pembuangan *virus definition* yang tidak digunakan.
5. Kesalahan yang terjadi pada *virus signature* akan ditolak oleh *addons* pada setiap perangkat lunak *antivirus*.

6.2 Saran

Saran yang penulis berikan sebagai pengembangan dari sistem *Universal Packet Update* ini sebagai berikut :

1. Pada sisi *server* dari sistem *Universal Packet Update* dapat dilakukan pemisahan *update packet* untuk masing-masing perangkat lunak *antivirus*, sehingga besar *update packet* yang harus di*download* oleh perangkat lunak *antivirus* dapat lebih kecil. Demikian juga dengan melakukan metode kompresi dengan algoritma yang telah ada seperti *Lempel-Zif* atau yang lainnya pada *update packet* untuk tujuan yang sama.
2. *Addons* dari perangkat lunak antivirus masih dapat dikembangkan lagi agar dapat melakukan *offline update* yang dapat memanfaatkan *update packet* yang disimpan pada direktori sementara ketika melakukan *online update* ke UPU Server sehingga *update packet* yang telah didapatkan dapat digunakan pada waktu yang berbeda dan oleh perangkat lunak antivirus yang juga berbeda.
3. Pengujian *Universal Packet Update* dapat dilakukan pada jaringan komputer yang lebih luas sehingga dapat diketahui secara lebih lengkap faktor-faktor yang akan mempengaruhi jalannya sistem *Universal Packet Update*.

Referensi

[1] Szor, Peter, 2005, *The Art of Computer Virus Research and Defense*, Addison Wesley, New York, USA.

[2] http://www.clamav.net/doc/webinars/Webinar-TK-2008-06-11.pdf diakses pada tanggal 10 Juli 2009 jam 17:05.

[3] http://id.wikipedia.org/MD5 diakses pada tanggal 10 Juli 2009 jam 17:05.

[4] http://n.wikipedia.org/wiki/List_of_computer_viruses diakses pada tanggal 25 Juli 2008 jam 17:05.

[5] http://www.clamav.net/ClamAV-developer.html diakses pada tanggal 10 Juli 2009 jam 17:05.

[6] http://www.clamav.net/doc/latest/signatures.pdf diakses pada tanggal 10 Juli 2009 jam 17:05.

[7] http://ivanlef0u.free.fr/repo/madchat/vxdevl/library/Creating%20*Antivirus*%20Signatures.pdf diakses pada tanggal 10 Juli 2009 jam 17:30.

[8] Drepper, Ulrich, at-all, 2008, *Linux Manual Page of MD5SUM*, Free Software Foundation, Inc.

[9] http://echo.or.id/forum/viewtopic.php?t=5903 diakses pada tanggal 6 Juli 2007.

[10] Team, 2007, *Linux Manual Page of Executable and Linking Format (ELF)*, Unix System Laboratories.

[11] Gailly, Jean, 2002, *Linux Manual Page of GZIP*, Free Software Foundation, Inc.

[12] Seward, Julian, *Linux Manual Page of BZIP2*, Free Software Foundation, Inc.