SPAM FILTERING DENGAN METODE REVERSE DNS LOOK UP (SPAM FILTERING WITH REVERSE DNS LOOK UP METHODE)

Nugroho[1], -[2]

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

Abstrak

Email merupakan layanan yang digunakan untuk berkorespondensi secara virtual melalui Internet. Kebutuhan untuk komunikasi yang mempunyai kemudahan, kecepatan, dan biaya yang murah sangat diperlukan dalam kehidupan masyarakat. Pengiriman email dari sender menuju recepient haruslah email yang benar tetapi saat ini banyak sekali email yang dikirim mempunyai tujuan tertentu, seperti untuk mengiklankan produk.

Ada dua jenis email yaitu ham dan spam. Ham adalah jenis email yang diharapkan sedangkan spam adalah jenis email yang mengganggu karena tidak diharapkan kedatangannya pada recipient atau hanya memenuhi queue di provider.

Salah satu metode spammer untuk mengirimkan spam dengan cara pemakaian IP Spoofing, menggunakan IP address dan domain orang lain. Penanggulangan untuk masalah ini dengan cara pengecekan kepemilikan IP address dengan domain-nya. Metode Reverse DNS Look Up merupakan solusi dari permasalahan IP Spoofing dengan optimalisasi bloking spam tetapi mempunyai kekurangan dalam filter email apabila IP address dan domain tidak terdaftar tetapi mengirimkan ham, maka akan terkena bloking juga.

Kata Kunci : Email, IP address dan domain, ham dan spam, Reverse DNS Look Up,

Abstract

Email represent a service for virtual correspondence on internet. Requirement of communications that has amenity, speed, and cheap expense is very needed in life of society. Delivery of email from sender to recipient must be a true email but in this time, a lot of delivery of email have another purpose, like offering of product.

There is two type of email that is ham and spam. Ham is a correct email but spam usually bother from recipient side which not expect email or fulfill email list allocation queue as well as provider side.

One of the method of spammer for delivery spam by use of IP Spoofing, IP address and domain others. The solution is by checking ownership of IP address with they domain. Method of Reverse DNS Look Up represents solution of problems of IP Spoofing with optimalitation spam blocking but they have lacking in email filter, if IP address and domain do not enlist but delivering ham, hence it will be hit by blocking filter too.

Keywords : Email,, IP address and domain, ham and spam, Reverse DNS Look Up,

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi pada saat ini mengalami perkembangan yang sangat pesat. Perkembangan teknologi informasi yang meliputi segala aspek kehidupan baik perkembangan suatu perusahaan maupun masyarakat. Salah satu teknologi informasi untuk bertukar komunikasi adalah *email*.

Electronicmail (*email*) merupakan suatu alat dengan teknologi elektronik yang sangat penting untuk komunikasi bagi setiap orang di era globalisasi sekarang ini. Ketepatan waktu pengiriman dan penerimaan *email* sangat diperlukan dan harus diperhatikan karena dapat mempengaruhi kehidupan seseorang atau suatu lembaga.

Layaknya seseorang menulis surat kepada orang lain melalui kantor pos dengan pengiriman yang bersifat biasa atau kilat, hanya saja mempunyai keterbatasan, salah satunya adalah masalah waktu. Oleh karena itu, diperlukan suatu alat yang berfungsi untuk komunikasi dengan kecepatan waktu pengiriman tinggi dan biaya yang murah.

Layanan *email* digunakan untuk berkorespondensi secara virtual melalui internet. Keuntungan *email* adalah kemudahan, murah secara ekonomis, serta kecepatan pengiriman yang cukup tinggi sehingga pengguna dapat berkorespondensi dengan orang lain yang berada di belahan bumi lainnya dengan cepat dan murah.

Pada saat layanan *email* banyak digunakan oleh masyarakat, ada jenis *email* yang mengganggu yang disebut *email spam*. Berbagai macam cara dilakukan *spammer* untuk mengirimkan *email spam* melalui jaringan internet, salah satunya dengan cara *IP Spoofing* – pemakaian *IP address* orang lain. Pemakaian *IP address* yang terdaftar adalah untuk mengelabui *anti-spam* yang berada di *server* agar kiriman *email* yang berupa *spam* dapat diteruskan ke penerima. Oleh karena itu, TA ini membahas bagaimana cara *blocking spam* dengan metode untuk menahan *IP address* palsu yaitu *Reverse DNS look Up*.

1.2 Perumusan Masalah

Adapun perumusan masalah dalam Tugas Akhir ini adalah sebagai berikut:

1. Bagaimana sistem dapat dibuat untuk mem-filter *email* yang dapat di-*drop* ketika *email* berada pada trafik *queue* jaringan pada *mail server*.
2. Bagaimana *mail server* mengetahui *IP address* dan *domain email* yang digunakan oleh *user* tersebut merupakan *IP address* dan *domain email* yang benar.
3. Bagaimana penerapan sistem *filtering* dapat membuat *queue* jaringan yang dilewati oleh *email*, dapat berjalan dengan lancar.

1.3 Tujuan

Tujuan Tugas Akhir ini adalah :

1. Membuat implementasi *library spam filtering* dengan menggunakan metode *Reverse DNS Look Up* dan menganalisis metode *Reverse DNS Look Up* sebagai metode *filtering* untuk *spam*.
2. Menganalisis *email* hasil *filtering* untuk melihat karakteristik *spam*.
3. Menganalisis perbandingan performansi hasil *filtering* pada *mail server* antara metode *Reverse DNS Look Up* dengan metode *Bayes* dilihat dari parameter hasil *filtering*.

1.4 Batasan Masalah

Dalam menganalisis permasalahan tersebut ada batasan pada beberapa *point*, antara lain :

1. Metode yang digunakan untuk memfilter *spam* adalah metode *Reverse DNS Look Up*.
2. Kegiatan analisis sistem *spam filtering* difokuskan pada kegiatan *email* pada *queue* di MTA.
3. Studi kasus pada TA ini dengan pemakaian *domain email* yang bersifat *private domain* karena keterbatasan kemampuan jaringan serta pembuatan *rule* spesifik.
4. Pemakaian *network address* yang tidak terlalu banyak, seperti -.-.-.-/30 (beberapa buah).

1.5 Metodologi Penelitian

Penelitian pada tugas akhir ini dilakukan dengan melalui beberapa cara , antara lain :

1. Studi literatur

   Dilakukan studi literatur atau tinjauan pustaka mengenai dasar-dasar konfigurasi *Mail Transfer Agent* dan *queue* pada trafik, serta mencari informasi yang berkaitan dengan proses *filtering spam* yang mendukung proses analisis dan perancangan ini.

2. Observasi

   Dilakukan observasi yang difokuskan pada

   - *Queue* untuk menganalisis *email*, serta data statistik mengenai kegiatan *email* di *queue*.
   - Metode *Reverse DNS Look Up* sebagai metode untuk memverifikasi dari *IP address* ke *domain email*.

3. Analisis metode *Reverse DNS Look Up* dan pembuatan *spam filter* dengan metode *Reverse DNS Look Up.*
4. Ujicoba *(testing)* terhadap sistem *spam filtering,* kemudian dilakukan evaluasi terhadap hasil yang telah dicapai dengan skenario *testing* di *email server.*
5. Terakhir, akan dilakukan perbandingan performansi hasil *filtering* dilihat dari parameter hasil *filtering.*

1.6 Sistematika Penulisan

Tugas Akhir ini disusun berdasarkan sistematika penulisan sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini akan dibahas tentang latar belakang penelitian, tujuan penelitian, perumusan masalah, pembatasan masalah, metode penelitian, dan sistematika penulisan tugas akhir

BAB II LANDASAN TEORI

Pada bab ini memuat berbagai dasar teori yang mendukung dan mendasari penulisan tugas akhir ini.

BAB III PERANCANGAN DAN IMPLEMENTASI

Pada bab ini dijelaskan perancangan dari program yang dibuat dan serangkaian proses umum berdasarkan mekanisme dan batasan yang digunakan.

BAB IV PENGUJIAN DAN HASIL ANALISIS

Pada bab ini akan dijelaskan pengujian dari skenario yang dibuat serta hasil analisis data – data yang diperoleh dari hasil percobaan yang menunjukkan kemampuan dan efektifitas proses.

BAB V KESIMPULAN DAN SARAN

Pada bab ini diberikan kesimpulan dari serangkaian penelitian yang dilakukan dan saran pengembangan selanjutnya.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Penerapan sistem *Spam Filtering* dengan menggunakan metode *Reverse DNS Look Up* cukup optimal apabila dijalankan untuk memfilter *email* yang *domain*-nya tidak terdaftar dan tidak sesuai dengan *IP address*-nya. Penerapan sistem dapat membuat trafik jaringan pada MTA berjalan semestinya (tidak memenuhi *space queue*) sehingga waktu pengiriman *email* tidak lama.

Dari hasil pengujian, penerapan sistem *Spam Filtering* dengan menggunakan metode *Reverse DNS Look Up* memberikan hasil, antara lain :

1. Spammer yang melakukan *IP spoofing* tidak berlaku lagi karena adanya pengecekan kepemilikan *IP address* terhadap *domain*-nya dilihat dari hasil uji coba skenario 3.
2. Mempunyai tingkat mem-*block email spam* diatas 94 % dari hasil uji coba skenario 4.
3. Waktu filter yang cukup cepat dengan rata-rata waktu yang relatif terhadap implementasi yang dibuat dengan spesifikasi *hardware* pada TA ini.
4. Ukuran dan jumlah *email* mempengaruhi waktu pemrosesan, semakin besar total ukuran *email* dan jumlah *email* maka semakin lama waktu pemrosesan *email filtering*.

Hanya saja penerapan sistem Spam Filtering dengan menggunakan metode *Reverse DNS Look Up* mempunyai sifat tidak efektif apabila email yang berisikan *ham* tetapi domain host tidak terdaftar harus di-*drop* oleh sistem.

Reverse DNS Look Up sering tidak bekerja dengan baik. Hal yang paling terlihat adalah banyaknya hasil yang bersifat *false negatif* sejak *Reverse DNS Look Up* dijalankan. Seperti contoh bila pemakaian *vanity domain names* yang tidak mempunyai *email server* tetapi berbagi dengan *email server hosting* perusahaan, seringkali ditolak karena mempunyai tingkat *false negatif* yang tinggi.

Solusi untuk meminimalisasi tingkat *false negatif* dengan membuat daftar domain yang "*trusted*" pada DNS *Server* atau dibuat *database*-nya.

5.2 Saran

1. Pengembangan sistem untuk *Spam Filtering* dengan menggunakan metode *Reverse DNS Look Up* haruslah mempunyai *database DNS* yang dapat didaftarkan pada organisasi pengelola DNS di internet seperti USENET.
2. Penerapan sistem untuk *Spam Filtering* lebih baik dengan penggabungan beberapa metode agar pengecekan *email* lebih akurat.
3. Penerapan sistem untuk *Spam Filtering* lebih baik dilakukan pada pengelola email (ISP) dengan kondisi yang nyata.
4. Pengolahan log dapat menggunakan *tools*, seperti Maia.

DAFTAR PUSTAKA

[1] Barracuda, An Overview of Spam Blocking Techniques, http://www.barracudanetworks.com/ns/downloads/barracuda_spam_blocking_techniques.pdf.

[2] Bautts, Tony, Terry Dawson, Gregor N. Purdy , *Linux Network Administrator's Guide*, ISBN 0-596-00548-2, 362 pages.Third Edition, February, 2005.

[3] Brent, D Chapman and Elizabeth D. Zwicky, *Building Internet Firewalls*, ISBN 1-56592-124-0, 517 pages,First Edition, November, 1995.

[4] Costales, Costales and Eric Allman, *Sendmail*, ISBN 1-56592-222-0, 1050 pages, Second Edition, January, 1997.

[5] Garfinkel, Simson and Gene Spafford, *Practical UNIX & Internet Security*, ISBN 1-56592-148-8, 1004 pages, Second Edition, April, 1996.

[6] Hunt, Craig, *TCP/IP Network Administration*, ISBN 1-56592-322-7, 630 pages, Second Edition, December, 1997.

[7] Jr, Frederick P. Brooks, *Wietse's Postfix Project*, Wietse Venema, IBM T.J. Watson Research, NY.

[8] *Linux Network Administrator's Guide, 3rd Edition*, is copyright © 2005 by O'Reilly & Associates.

[9] Liu, Cricket and Paul Albitz, *DNS & BIND*, ISBN 1-56592-512-2, 502 pages. Third Edition, September, 1998.

[10] Purbo, Onno.W, *TCP/IP*, ISBN-979-20-0759-8, 378 halaman. Edisi Pertama, September, 1998.

[11] Tarigan, I Made Wiryana Avinanta, *Analyzing Security Incidents with Why Because Analysis*, Bieleschweig Workshop - System Safety, German Chapter of System Safety, December 2002.

[12] Tezar, Asmed, *Implementasi Spamasssin sebagai Anti-Spam pada Sistem Email di PT. Badak NGL*, STT Telkom, September, 2005.

[13] *The Networking CD Bookshelf*, version 1.0, is copyright © 1999 by O'Reilly & Associates .