IMPLEMENTASI FUZZY HASHING UNTUK MENINGKATKAN JUMLAH DETEKSI MALWARE DENGAN METODE SIGNATURE BASED DETECTION

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer (S.Kom.)

Aditia Rinaldi

11110110060

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INFORMASI DAN KOMUNIKASI

UNIVERSITAS MULTIMEDIA NUSANTARA

TANGERANG

2015

PERNYATAAN TIDAK MELAKUKAN PLAGIAT

Dengan ini, saya:

Nama : Aditia Rinaldi

NIM : 11110110060

Fakultas : Teknologi Informasi dan Komunikasi

Program Studi : Teknik Informatika

menyatakan bahwa skripsi yang berjudul IMPLEMENTASI FUZZY HASHING UNTUK MENINGKATKAN JUMLAH DETEKSI MALWARE DENGAN METODE SIGNATURE BASED DETECTION ini adalah karya ilmiah saya sendiri, bukan plagiat dari karya ilmiah yang ditulis oleh orang lain atau lembaga lain, dan semua karya ilmiah orang lain atau lembaga lain yang dirujuk dalam skripsi ini telah disebutkan sumbernya serta dicantumkan di Daftar Pustaka.

Jika di kemudian hari terbukti ditemukan kecurangan/penyimpangan, baik dalam pelaksanaan skripsi maupun dalam penulisan laporan skripsi, saya bersedia menerima konsekuensi dinyatakan TIDAK LULUS untuk mata kuliah Skripsi yang telah saya tempuh.

Tangerang, 27 April 2015

(Aditia Rinaldi)

LEMBAR PENGESAHAN SKRIPSI

IMPLEMENTASI FUZZY HASHING UNTUK MENINGKATKAN JUMLAH DETEKSI MALWARE DENGAN METODE SIGNATURE BASED DETECTION

Oleh

Nama : Aditia Rinaldi

NIM : 11110110060

Fakultas : Teknologi Informasi dan Komunikasi

Program Studi : Teknik Informatika

Tangerang, 7 Mei 2015

Ketua Sidang	Dosen Penguji
Maria Irmina Prasetiyowati, S.Kom., M.T.	Ranny, S.Kom., M.Kom.
Dosen Pembimbing I	Dosen Pembimbing II
Yustinus Widya Wiratama, S.Kom., M.Sc.	Seng Hansun, S.Si., M.Cs.

Mengetahui,

Ketua Program Studi Teknik Informatika

Maria Irmina Prasetiyowati, S.Kom., M.T.

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Sempurna atas berkat, kekuatan, serta limpahan inspirasi-Nya sehingga penulis dapat menyelesaikan skripsi beserta penulisan laporannya yang merupakan salah satu tahap bersejarah dalam perjalanan panjang pendidikan. Laporan ini dipersiapkan untuk diajukan kepada Program Studi Teknik Informatika, Fakultas Teknologi Informasi dan Komunikasi, Universitas Multimedia Nusantara sebagai salah satu syarat kelulusan memperoleh gelar Sarjana Komputer (S.Kom.).

Terselesaikannya skripsi ini tidak lepas dari kerja sama banyak pihak, untuk itu izinkan penulis mengucapkan terima kasih kepada:

1. Dr. Ninok Leksono, Rektor Universitas Multimedia Nusantara,
2. Kanisius Karyono, S.T., M.T., Dekan Fakultas Teknologi Informasi dan Komunikasi Universitas Multimedia Nusantara,
3. Maria Irmina Prasetiyowati, S.Kom., M.T., Ketua Program Studi Teknik Informatika Universitas Multimedia Nusantara dan selaku ketua sidang skripsi yang telah memberi masukan dalam menulis skripsi,
4. Yustinus Widya Wiratama, S.Kom., M.Sc. dan Seng Hansun, S.Si., M.Cs. yang membimbing pembuatan skripsi dan yang telah mengajar penulis tata cara menulis karya ilmiah dengan benar,
5. Ranny, S.Kom., M.Kom. selaku penguji dalam sidang skripsi yang telah memberi masukan dalam menulis skripsi,
6. Keluarga penulis yang telah memberikan dukungannya,
7. Segenap dosen, dan teman penulis yang tidak dapat penulis sebutkan satu-persatu.

Semoga skripsi ini bisa bermanfaat untuk memberikan informasi yang berguna dan menjadi inspirasi bagi seluruh pembacanya.

Tangerang, 27 April 2015

(Aditia Rinaldi)

IMPLEMENTASI FUZZY HASHING UNTUK MENINGKATKAN JUMLAH DETEKSI MALWARE DENGAN METODE SIGNATURE BASED DETECTION

ABSTRAK

Hash tradisional yang umum digunakan adalah MD5, SHA-1, dan SHA256. Dalam penelitian ini, keterbatasan *hash* tradisional dimana nilainya digunakan untuk membandingkan kesamaan *file* (*fingerprinting*), akan digantikan dengan *fuzzy hashing* sebagai salah satu metode *hash* yang berbeda dari *hash* tradisional karena dengan menggunakan *fuzzy hash* dapat mendeteksi kemiripan *file* dengan *output* berupa rentang nilai dari nol (tidak mirip) sampai dengan satu (sangat mirip) sehingga *malware* yang dapat terdeteksi dapat melebihi jumlah *signature* yang telah ada dalam *database* walau *signature malware* sebenarnya belum dibangun ke dalam *database*, terutama *malware* yang masih mirip atau varian dari *malware* yang telah terdapat dalam *database* dengan batas toleransi kemiripan minimal (*threshold*) tertentu. Implementasi *fuzzy hashing* menggunakan gabungan algoritma *spamsum* untuk menghasilkan nilai *hash* dan algoritma *Levenshtein Distance* termodifikasi untuk membandingkan kemiripan antara dua nilai *fuzzy hash*. Dari hasil uji coba, didapati bahwa implementasi *fuzzy hashing* pada *signature malware* dapat meningkatkan jumlah deteksi *malware* rata-rata sebesar 31,84% dan meningkatkan tingkat akurasi rata-rata sebesar 16,63% dari *hash* tradisional SHA256. Peningkatan jumlah deteksi dan akurasi optimal dapat dicapai pada *threshold* 50%.

Kata kunci: *accuracy*, *detection rate*, *fuzzy hasing*, *signature-based detection*, *signature malware*.

IMPLEMENTATION OF FUZZY HASHING TO INCREASE THE NUMBER OF MALWARE DETECTION WITH SIGNATURE-BASED DETECTION METHOD

ABSTRACT

Traditional hash that commonly used is MD5, SHA-1, and SHA256. In this research, the limitations of traditional hash where the value is used to compare identical file (fingerprinting), will be replaced by fuzzy hashing as one of the hash method that slightly different from traditional hash because by using fuzzy hash can detect similaritiy with output value from zero (not similar) to one (very similar), so the number of detected malware can exceed the number of signatures that have been stored in database eventhough the actual malware signatures have not been built or stored in the database, especially similar malware or variant of malware that have been stored in the database with specific threshold. Implementation of fuzzy hash use a combination spamsum algorithm to generate fuzzy hash value and modified Levenshtein Distance algorithm to compare similarity between two fuzzy hash value. And the result, the implementation of fuzzy hashing on malware signature can increase the number of malware detection on average by 31,84% and increase the accuracy rate on average by 16,63% from SHA256 traditional hash. Optimal enhancement number of malware detection and accuracy rate can be achieved at the threshold 50%.

Keywords: accuracy, detection rate, fuzzy hasing, signature-based detection, signature malware.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR