

**PERBANDINGAN KEAMANAN MEMORY/PROCESSOR
HUNGRY PASSWORD BASED KEY DERIVATION FUNCTION
DENGAN TEKNIK PENYIMPANAN PASSWORD ENKRIPSI,
HASH DAN HASH+SALT**

TESIS



Oleh:

Muhammad Yusuf Bambang Setiadji
0911600187

**PROGRAM STUDI : MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR**

**JAKARTA
2013**

**PERBANDINGAN KEAMANAN MEMORY/PROCESSOR
HUNGRY PASSWORD BASED KEY DERIVATION FUNCTION
DENGAN TEKNIK PENYIMPANAN PASSWORD ENKRIPSI,
HASH DAN HASH+SALT**

TESIS

**Diajukan untuk memenuhi salah satu persyaratan
memperoleh gelar Magister Komputer**



Oleh

Muhammad Yusuf Bambang Setiadji
0911600187

**PROGRAM STUDI : MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR**

**JAKARTA
2013**



LEMBAR PENGESAHAN

Nama : Muhammad Yusuf Bambang Setiadji
Nomor Induk Mahasiswa : 0911600187
Konsentrasi : Rekayasa E-Business
Jenjang Studi : Strata 2
Judul : Perbandingan Keamanan *Memory/Processor*
Hungry Password Based Key Derivation
Function Dengan Teknik Penyimpanan
Password Enkripsi, Hash Dan Hash+Salt

Jakarta, 23 Februari 2013

Tim Penguji:

Tanda tangan:

Ketua,
Dr. Ir. Nazori AZ, M.T.

Anggota,
Dr. Moedjiono, M.Sc

Pembimbing,
Dr. Ir. Nazori AZ, M.T.

Pembimbing Pendamping
Mardi Hardjianto, M.Kom

Ketua Program Studi

Dr. Ir. Nazori AZ, M.T.



LEMBAR PERNYATAAN

Saya yang bertanda tangan dibawah ini :

Nama : Muhammad Yusuf Bambang Setiadi
NIM : 0911600187
Program : Magister Ilmu Komputer
Studi :
Program : Rekayasa E-Business

menyatakan bahwa TESIS yang berjudul:

Perbandingan Keamanan Memory / Processor
Hungry Password Based Key Derivation Function
Dengan Teknik Penyimpanan Password Enkripsi,
Hash dan Hash + Salt

1. merupakan hasil karya tulis ilmiah sendiri dan bukan merupakan karya yang pernah diajukan untuk memperoleh gelar akademik oleh pihak lain,
2. saya ijin untuk dikelola oleh Universitas Budi Luhur sesuai dengan norma hukum dan etika yang berlaku.

Pernyataan ini saya buat dengan penuh tanggung jawab dan saya bersedia menerima konsekuensi apapun sesuai aturan yang berlaku apabila di kemudian hari pernyataan ini tidak benar.

Jakarta, 1 Maret 2013


()
M. Yusuf B S

Abstrak

Metode otentikasi merupakan cara yang digunakan untuk mengamankan data/informasi sensitif dari pengguna yang tidak berhak. Proses *login* situs *on-line* maupun *login* pada komputer merupakan dua contoh penerapan metode otentikasi. Metode otentikasi yang umum adalah menggunakan kombinasi *username - password*. Metode otentikasi ini didasarkan pada sesuatu yang diketahui oleh pengguna, yaitu sebuah *password*. Cara kerja metode otentikasi ini adalah membandingkan *username-password* yang diisikan oleh pengguna dengan data *username-password* yang disimpan dalam basis data situs *on-line* maupun komputer tersebut. Dengan demikian *password* merupakan data sensitif yang penyimpanannya harus diamankan sebaik mungkin. Perkembangan teknologi informasi telah melahirkan beberapa teknik kriptografi yang dapat digunakan untuk mengamankan data *password* tersebut. Penelitian ini akan membandingkan keamanan beberapa teknik tersebut, diantaranya adalah enkripsi, *hash*, *hash+salt* dan *password based key derivation function*. Dengan demikian akan didapat teknik penyimpanan terbaik yang sesuai dengan perkembangan teknologi informasi saat ini.

Kata kunci : otentikasi, kriptografi, *password*, *hash*, MD5, *key derivation function*

Abstract

Authentication method is a way that is used to protect sensitive data or information from unauthorized access. Login process in on-line sites or login on computer are two examples of common use of authentication method. A typical type of authentication method is the use of username and password combination. This type of authentication method is based by comparing the username-password that the user inputs to the username-password that is stored in the database of on-line sites or computer. In such manner, password are sensitive data that are supposed to be protected as good as possible. The development of information technology has given birth to several cryptographic technique in securing the password data. This research will compare the security of said technique, including encryption, hash, hash+salt and password based key derivation function. Thus, this research is to conclude the best technique that are suitable with the development of information technology.

Keywords : authentication, cryptography, password, hash, MD5, key derivation function

KATA PENGANTAR

Assalamualaikum Warrahmatullahi Wabarokatuh,

Puji syukur marilah selalu kita panjatkan atas kehadiran Allah SWT, karena hanya dengan kehendak-Nya tesis tentang " Perbandingan Keamanan *Memory/Processor Hungry Password Based Key Derivation Function* Dengan Teknik Penyimpanan Password Enkripsi, *Hash* Dan *Hash+Salt* " ini dapat diselesaikan. Dalam penyusunan tesis ini, penulis mengucapkan terimakasih kepada :

1. Allah SWT, atas segala rahmat dan ridhonya yang selalu menyertai semua aktifitas penulis;
2. Kepala Program Studi Magister Komputer, Universitas Budi Luhur;
3. Bapak Dr. Ir. Nazori A.Z.,M.T. dan Bapak Mardi Hadjrianto M.Kom selaku pembimbing;
4. Ayu Pustikasari dan Aira Yudika Setiadji, yang selalu memberikan inspirasi;
5. Kedua orangtua dan kakak adik saya atas semua dukungan serta doanya;
6. Serta semua pihak yang tidak dapat dituliskan.

Sebagai seorang manusia yang selalu memiliki kekurangan, penulis menyadari bahwa tesis ini masih memiliki banyak kekurangan, oleh karena itu segala bentuk saran dan kritik mohon dikirimkan melalui email ke alamat muhammad.yusuf@lemsaneg.go.id.

Wassalamualaikum Warahmatullahi Wabarakatuh

Jakarta, Februari 2013

M. Yusuf Bambang Setiadji

DAFTAR ISI

	Halaman
ABSTRAK	ii
ABSTRACT	iii
KATA PENGANTAR	iv
DAFTAR ISI	v
DAFTAR GAMBAR	vii
DAFTAR TABEL	viii
BAB I PENDAHULUAN	
1.1. Latar Belakang.....	1
1.2. Masalah Penelitian.....	4
1.3. Tujuan dan Manfaat Penelitian.....	6
1.4. Sistematika Penelitian.....	6
1.5. Daftar Istilah.....	7
BAB II TINJAUAN TEORI DAN PENGEMBANGAN HIPOTESIS	
2.1. Tinjauan Teori	9
2.1.1. Letak Keamanan Kriptografi	9
2.1.2. Kriptografi	10
2.1.3. Manajemen Password.....	10
2.1.4. Secure Hash Algorithm	17
2.1.5. Password-Based Key Derivation Function.....	32
2.2. Kajian Literatur	35
2.2.1. Making a Faster Cryptanalytic Time-Memory Trade-Off.....	35
2.2.2. GPU-Based Password Cracking	43
2.2.3. BCRYPT.....	51
2.2.4. SCRYPT	53
2.3. Tinjauan Objek Penelitian.....	55
2.4. Kerangka Konsep	56
2.5. Hipotesis Penelitian	59

BAB III METODOLOGI PENELITIAN	
3.1. Metode Penelitian	61
3.2. Operasionalisasi Variabel.....	62
3.3. Data dan Sumber Data	63
3.4. Teknik Pengumpulan Data.....	63
3.5. Rancangan Analisis dan Uji Hipotesis.....	64
3.6. Langkah - Langkah Penelitian.....	67
3.7. Jadwal Penelitian	68
BAB IV ANALISIS DATA DAN PEMBAHASAN HASIL PENELITIAN	
4.1. Hasil Penelitian.....	69
4.2. Analisis Keamanan pada Penyimpanan Password	74
4.3. Faktor Keamanan <i>bcrypt</i> dan <i>scrypt</i>	77
4.4. Implikasi Penelitian	78
4.5. Rencana Implementasi.....	80
BAB V KESIMPULAN DAN SARAN	
5.1. Kesimpulan	82
5.2. Saran	83
DAFTAR PUSTAKA	84
LAMPIRAN - Screenshot Proses Pemecahan Password.....	86

DAFTAR GAMBAR

Gambar	Halaman
I.1. Proses mengakses situs dengan akses kontrol.....	3
II.1. Taksonomi Kriptografi	11
II.2. Diagram PBKDF	33
II.3. Diagram Umum PBKDF2	35
II.4. Desain CPU dan GPU.....	44
II.5. Kerangka Konsep	58
III.1. Keterkaitan Antar Dua Variabel.....	62
III.2. Rancangan Analisis	64
IV.1. Baris Perintah Dictionary Attack oclhashcat-plus	70
IV.2. Baris Perintah GRT-RainbowCrack.....	71
IV.3. Baris Perintah oclhachcat-plus.....	74
IV.4. Ilustrasi Lokasi Memori Penyimpanan.....	78

DAFTAR TABEL

Tabel	Halaman
II.1. Tabel Kemungkinan <i>Keyspace</i>	16
II.2. Gambaran Dasar Algoritma Hash	19
II.3. Perbedaan Antara Tabel Klasik Dengan <i>Rainbow Tables</i>	40
II.4. Perbandingan Tingkat Kesuksesan.....	41
II.5. Tabel Statistik Perbandingan Tabel Klasik Dengan <i>Rainbow Tables</i>	42
II.6. Skema MD5-crypt	49
II.7. Perbandingan Kecepatan Antar Optimasi Skema MD5-Crypt	50
II.8. Karakteristik Kelas dan Jumlah Password.....	51
II.9. Pencarian Menyeluruh Terhadap Empat Kelas Password	51
II.10. Perbandingan Kajian Literatur	55
III.1. Skema Langkah-Langkah Penelitian.....	67
IV.1. Perbandingan Pemecahan Dengan <i>Wordlist</i>	69
IV.2. Jumlah Komputasi <i>rainbow table</i>	71
IV.3. CPU <i>brute-force</i>	73
IV.4. GPU <i>brute-force</i>	74
IV.5. Perbandingan Waktu Pemecahan	75
IV.6. Hubungan Jumlah Komputasi - Waktu Pencarian Maksimal	75
IV.7. <i>Timeline</i> Susunan Rencana Implementasi	81

DAFTAR PUSTAKA

- [Federal Financial Institution Examination Council, 2001] Federal Financial Institution Examination Council. (2001, August). Authentication in an Electronic Banking Environment.
- [FED-STD-1037C] Federal Information Processing Standards. (2012). *Secure Hash Standards*. FIPS Publication, National Institute of Standards and Technology, Gaithersburg. FED-STD-1037C. (t.thn.). Institute Telecommunication Glossary.
- [Hasibuan, 2007] Hasibuan, Z. A. (2007). *Metodologi Penelitian pada Bidang Ilmu Komputer dan Teknologi Informasi*. Depok: Universitas Indonesia.
- [Hellman, 1980] Hellman, M. E. (1980). A Cryptanalytic Time-Memory Trade-Off. *IEEE Transaction On Information Theory* , IT-26.
- [Istiyanto & Widodo, 2009] Istiyanto, J. E., & Widodo, A. P. (2009). Karakteristik Metodologi Penelitian Bidang Ilmu Komputer (IK) Berlandaskan Pendekatan Positivistik. *Jurnal Sains dan Matematika (JSM)* , 17.
- [Kerckhoffs, 1883] Kerckhoffs, A. (1883). La Cryptographie Militaire. *Journal des sciences militaires* , IX, 5-38.
- [Menezes, Oorschot, & Vanstone, 1996] Menezes, A. J., Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. Massachusets: CRC Press.
- [Mironov, 2005] Mironov, I. (2005). *Hash Functions : Theory, Attacks, and Applications*. Survey, Microsoft Research, Silicon Valley.
- [Oechslin, 2003] Oechslin, P. (2003). Making a Faster Cryptanalytic Time-Memory Trade-Off. *Crypto 2003*. Santa Barbara.
- [Percival, 2009] Percival, C. (2009). Stronger Key Derivation Via Sequential Memory-Hard Functions. *BSDCan - The BSD Conference*. Ottawa: BSDCan.
- [Privacy Rights Clearinghouse, 2011] Privacy Rights Clearinghouse. (2011, December). Data Breaches: A Year in Review.