Perpustakaan Universitas Budi Luhur

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

Perpustakaan Universitas Budi Luhur

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

Perpustakaan Universitas Budi Luhur

LEMBAR PENGESAHAN

Nama	: Muhammad Yusuf Bambang Setiadji
Nomor Induk Mahasiswa	: 0911600187
Konsentrasi	: RekayasaE-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.

Perpustakaan Universitas Budi Luhur

LEMBAR PERNYATAAN

Saya yang bertanda tangan dibawah ini :

Nama : Muhammad Yusuf Bambang Setiadji

NIM : 0911600187

Program Studi : Magister Ilmu Komputer

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 ijinkan 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 BS)

Perpustakaan Universitas Budi Luhur

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*

Perpustakaan Universitas Budi Luhur

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

Perpustakaan Universitas Budi Luhur

KATA PENGANTAR

Assalamualaikum Warrahmatullahi Wabarokatuh,

Puji syukur marilah selalu kita panjatkan atas kehadirat 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

Perpustakaan Universitas Budi Luhur

DAFTAR ISI

Halaman

Perpustakaan Universitas Budi Luhur

Perpustakaan Universitas Budi Luhur

DAFTAR GAMBAR

Gambar Halaman

Perpustakaan Universitas Budi Luhur

DAFTAR TABEL

Tabel Halaman

Perpustakaan Universitas Budi Luhur

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 Telecomunication 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.